



# Documentação do Active IQ Unified Manager

Active IQ Unified Manager 9.16

NetApp  
November 19, 2024

# Índice

Documentação do Active IQ Unified Manager	1
Notas de lançamento	2
Comece agora	3
Instruções de início rápido para instalações VMware	3
Instruções de início rápido para instalações Linux	4
Instruções de início rápido para instalações do Windows	5
Instale o Unified Manager nos sistemas VMware vSphere	7
Introdução ao Active IQ Unified Manager	7
Requisitos para instalar o Unified Manager	8
Instalação, atualização e remoção do software Unified Manager	16
Instale o Unified Manager em sistemas Linux	25
Introdução ao Active IQ Unified Manager	25
Requisitos para instalar o Unified Manager	26
Instalação, atualização e remoção do software Unified Manager	35
Instale o Unified Manager em sistemas Windows	56
Introdução ao Active IQ Unified Manager	56
Requisitos para instalar o Unified Manager	57
Instalação, atualização e remoção do software Unified Manager	66
Executar tarefas de configuração e administrativas	77
Configurando o Active IQ Unified Manager	77
Configuração do backup do Unified Manager	97
Gerir definições de funcionalidades	97
Utilizar a consola de manutenção	101
Gerenciando o acesso do usuário	115
Gerenciando configurações de autenticação SAML	121
Gerenciamento da autenticação	128
Gerenciamento de certificados de segurança	135
Monitorar e gerenciar o storage	142
Introdução ao Active IQ Unified Manager	142
Compreender a interface do utilizador	145
Monitoramento e gerenciamento de clusters no painel	152
Gerenciamento de clusters	164
Monitoramento da infraestrutura virtual VMware	169
Provisionamento e gerenciamento de workloads	179
Gerenciamento e monitoramento de configurações do MetroCluster	196
Gerenciamento de cotas	204
Solução de problemas	211
Gerenciar eventos e alertas	218
Gerenciamento de eventos	218
Gerenciamento de alertas	314
Gerenciamento de scripts	328
Monitorar e gerenciar o desempenho do cluster	338
Introdução ao monitoramento de desempenho do Active IQ Unified Manager	338

Navegando em workflows de performance na GUI do Unified Manager . . . . .	342
Monitoramento do desempenho do cluster no Dashboard . . . . .	352
Solução de problemas de cargas de trabalho usando o analisador de carga de trabalho . . . . .	354
Monitoramento do desempenho do cluster na página de destino do cluster de desempenho . . . . .	357
Monitorando o desempenho usando as páginas Inventário de desempenho . . . . .	363
Monitoramento do desempenho usando as páginas do Performance Explorer . . . . .	373
Gerenciando o desempenho usando informações de grupo de políticas de QoS . . . . .	395
Gerenciamento da performance com a capacidade de performance e as informações de IOPS disponíveis . . . . .	401
Compreender e utilizar a página Planeamento de failover de nó . . . . .	410
Coleta de dados e monitoramento do desempenho da carga de trabalho . . . . .	414
Compreender eventos e alertas de desempenho . . . . .	423
Gerenciamento dos limites de performance . . . . .	434
Analisando eventos de desempenho . . . . .	445
Resolução de eventos de performance . . . . .	460
Configurando uma conexão entre um servidor do Unified Manager e um provedor de dados externo . . . . .	475
Monitorar e gerenciar a integridade do cluster . . . . .	480
Introdução ao monitoramento da saúde do Active IQ Unified Manager . . . . .	480
Gerenciamento e monitoramento de clusters e integridade de objetos do cluster . . . . .	483
Tarefas e workflows de integridade do Unified Manager comuns . . . . .	497
Proteger e restaurar dados . . . . .	627
Criação, monitoramento e solução de problemas de relacionamentos de proteção . . . . .	627
Gerenciamento e monitoramento de relações de proteção . . . . .	640
Gerar relatórios personalizados . . . . .	719
Relatórios do Unified Manager . . . . .	719
Trabalhando com relatórios . . . . .	724
Agendar relatórios . . . . .	732
Exemplos de relatórios personalizados . . . . .	737
Exemplos de relatórios do Microsoft Excel . . . . .	755
Gerenciar o storage usando APIS REST . . . . .	767
Primeiros passos com as APIS REST do Active IQ Unified Manager . . . . .	767
Acesso à API REST e autenticação no Active IQ Unified Manager . . . . .	771
APIs REST do Unified Manager . . . . .	781
Workflows de API comuns para gerenciamento de storage . . . . .	818
Avisos legais . . . . .	852
Direitos de autor . . . . .	852
Marcas comerciais . . . . .	852
Patentes . . . . .	852
Política de privacidade . . . . .	852
Código aberto . . . . .	852

# Documentação do Active IQ Unified Manager

# Notas de lançamento

Fornece um resumo de novos recursos, limitações e problemas conhecidos do Active IQ Unified Manager 9,16.

Para obter mais informações, consulte ["Notas de versão do Active IQ Unified Manager"](#) .

# Comece agora

## Instruções de início rápido para instalações VMware

Você pode baixar o `.tar` arquivo que contém um certificado raiz, um README arquivo e um OVA arquivo e implantar o Unified Manager como um dispositivo virtual.

### Requisitos do sistema

- Sistema operacional: VMware ESXi 7,0 e 8,0
- RAM: 12 GB
- CPU: Total de 9572 MHz
- Espaço livre em disco: 5 GB (provisionamento fino), 152 GB (provisionamento espesso)

Para obter os requisitos detalhados do sistema, consulte ["Requisitos para instalar o Unified Manager"](#) e ["Matriz de interoperabilidade"](#).

## A instalar o Active IQ Unified Manager

### Baixe o instalador

1. Baixe o `.tar` arquivo que contém um certificado raiz, um README arquivo e um OVA arquivo.
2. Salve o arquivo em um diretório local ou diretório de rede acessível ao cliente vSphere.
3. No diretório em que você baixou o `.tar` arquivo, digite o `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz` comando. O arquivo necessário OVA, um certificado de raiz e um README arquivo são descompactados para o diretório de destino.

### Verifique a integridade

Você pode verificar a integridade OVA do arquivo seguindo as etapas fornecidas no README arquivo.

### Instale o Unified Manager

1. No vSphere Client, clique em **File > Deploy OVF Template**.
2. Localize o arquivo OVA e use o assistente para implantar o dispositivo virtual no servidor ESXi.
3. Na página Detalhes da revisão, na seção Editor, a mensagem `Entrust Code Signing - OVCS2 (Trusted certificate)` confirma a integridade do arquivo baixado OVA. Para a mensagem `Entrust Code Signing - OVCS2 (Invalid certificate)`, atualize o VMware vCenter Server para a versão 7.0U3E ou superior.
4. Na página Personalizar modelo, na guia Propriedades, preencha os campos conforme necessário para o tipo de instalação que você está executando:
  - Para a configuração estática, introduza as informações necessárias em todos os campos. Adicionar informações para o campo **DNS secundário** não é necessário.
  - Para DHCP usando IPv4, não adicione nenhuma informação em nenhum campo.
  - Para DHCP usando IPv6, marque a caixa "Ativar endereçamento IPv6 automático". Não adicione nenhuma informação em nenhum outro campo.

5. Ligue a VM.
6. Clique na guia Console para exibir o processo de inicialização inicial.
7. Configure o fuso horário.
8. Introduza um nome de utilizador e uma palavra-passe de manutenção do Unified Manager.

No final da instalação, as informações para se conectar à IU da Web do Unified Manager são exibidas.

## Instruções de início rápido para instalações Linux

Você pode baixar o pacote de instalação e instalar o Unified Manager em uma plataforma física ou virtual Red Hat Enterprise Linux.

### Requisitos do sistema

- Sistema operacional: Red Hat Enterprise Linux versões 8.x e 9.4, baseado na arquitetura x86\_64, instalado usando o ambiente base "servidor com GUI" da opção **seleção de Software** do instalador do SO
- RAM: 12 GB, CPU: 9572 MHz total
- Espaço livre em disco: 100 GB de espaço em disco no `/opt/netapp/data` diretório, 50 GB na partição raiz. Para diretórios e `/var/log` montados separadamente `/opt`, certifique-se de que `/opt` tem 15 GB, `/var/log` tem 16 GB e `/tmp` tem 10 GB de espaço livre.

Para obter informações detalhadas sobre os requisitos do sistema e sobre a instalação do produto em um local seguro, consulte ["Requisitos para instalar o Unified Manager"](#) e o ["Matriz de interoperabilidade"](#).

## A instalar o Active IQ Unified Manager

### Baixe o instalador

1. Faça o download do `ActiveIQUnifiedManager-<version>.zip` pacote de instalação juntamente com o certificado de assinatura de código (`.pem`) e a assinatura digital (`.sig`).
2. No diretório em que você baixou o arquivo de instalação, execute:

```
# unzip ActiveIQUnifiedManager-<version>.zip
```

### Verifique a integridade

Execute os seguintes comandos para verificar a integridade do pacote de instalação:

- Execute `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>` para criar um arquivo com a chave pública a partir do certificado de assinatura de código.
- Execute `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip` para verificar a assinatura no pacote do instalador.

### Verifique a configuração do repositório

Os procedimentos para configurar um repositório Red Hat Enterprise Linux são específicos do site. Você pode

usar o `pre_install_check.sh` script incluído no pacote de instalação para verificar a configuração do seu sistema operacional. Se o seu sistema estiver conectado à Internet, você receberá automaticamente instruções para configurar o repositório Red Hat Enterprise Linux.

```
# sudo ./pre_install_check.sh
```

## Instale o Unified Manager

O Unified Manager usa `yum` o utilitário para instalar o software e qualquer software dependente. Como existem várias imagens do Red Hat Enterprise Linux, os pacotes instalados dependem do software presente nas imagens. O `yum` utilitário determina os pacotes de software dependentes para instalação. Se precisar de mais informações sobre os pacotes de software dependentes, consulte o ["Requisitos de software e instalação do Linux"](#).

Para instalar o Unified Manager, execute o seguinte comando, como usuário raiz ou usando `sudo`, no diretório em que o arquivo de instalação foi descompactado:

```
# yum install netapp-um<version>.x86_64.rpm
```

ou

```
% sudo yum install netapp-um<version>.x86_64.rpm
```

No final da instalação, as informações para se conectar à IU da Web do Unified Manager são exibidas. Se você não conseguir se conectar à IU da Web, consulte o `README` arquivo empacotado com o software para obter mais informações sobre as restrições da porta 443.

## Instruções de início rápido para instalações do Windows

Você pode baixar o pacote de instalação e instalar o Unified Manager para monitorar e solucionar problemas de capacidade, disponibilidade, performance e proteção de storage de dados.

### Requisitos do sistema

- Sistemas operacionais
  - Microsoft Windows Server 2019 Standard e Datacenter Edition
  - Microsoft Windows Server 2022 Standard e Datacenter Edition

O Unified Manager é compatível com o sistema operacional Windows de 64 bits para os seguintes idiomas:

- Inglês
  - Japonês
  - Chinês simplificado
- RAM: 12 GB
  - CPU: Total de 9572 MHz
  - Espaço livre em disco: 100 GB de espaço em disco para o diretório de instalação, 50 GB de espaço em disco para o diretório de dados MySQL



Para obter os requisitos detalhados do sistema, consulte ["Requisitos para instalar o Unified Manager"](#) e ["Matriz de interoperabilidade"](#).

## A instalar o Active IQ Unified Manager

### Baixe o instalador

1. Baixe o `ActiveIQUnifiedManager-<version>.exe` pacote de instalação.
2. Copie o arquivo de instalação para um diretório no sistema de destino.

### Instale o Unified Manager

Para instalar o Unified Manager, certifique-se de que tem o Microsoft .NET 4,5.2 ou uma versão posterior instalada. Como parte do processo de instalação, o Unified Manager instala outros pacotes de terceiros, conforme necessário. Para obter mais informações sobre os pacotes de software dependentes, consulte o ["Requisitos de software e instalação do Windows"](#).

1. Inicie sessão no Windows utilizando a conta de administrador local predefinida.
2. No diretório em que você baixou o arquivo de instalação, clique com o botão direito do Mouse e execute o arquivo executável do Unified Manager (.exe) como administrador.
3. Quando solicitado, insira o nome de usuário e a senha para criar o usuário de manutenção do Unified Manager.
4. No assistente conexão de banco de dados, insira a senha raiz do MySQL.
5. Siga as instruções restantes para concluir a instalação.
6. Clique em **Finish** no final da instalação e a IU da Web do Unified Manager será exibida.

# Instale o Unified Manager nos sistemas VMware vSphere

## Introdução ao Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente chamado Gerenciador Unificado de OnCommand) permite que você monitore e gerencie a integridade e a performance dos sistemas de storage da ONTAP com uma única interface. Você pode implantar o Unified Manager em um servidor Linux, em um servidor Windows ou como um dispositivo virtual em um host VMware.

Após concluir a instalação e adicionar os clusters que você deseja gerenciar, o Unified Manager fornece uma interface gráfica que exibe a capacidade, disponibilidade, proteção e status de performance dos sistemas de storage monitorados.

### Informações relacionadas

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

### O que o servidor Unified Manager faz

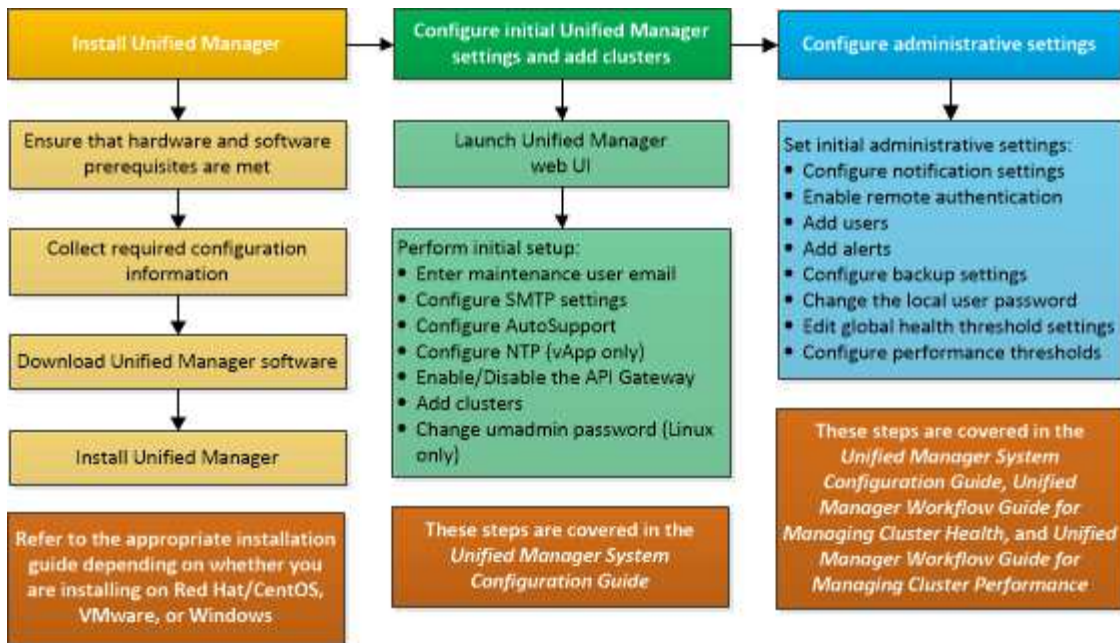
A infraestrutura de servidor do Unified Manager consiste em uma unidade de coleta de dados, um banco de dados e um servidor de aplicativos. Ele fornece serviços de infraestrutura como descoberta, monitoramento, controle de acesso baseado em funções (RBAC), auditoria e logs.

O Unified Manager coleta informações de cluster, armazena os dados no banco de dados e analisa os dados para verificar se há problemas de cluster.

### Descrição geral da sequência de instalação

O fluxo de trabalho de instalação descreve as tarefas que você deve executar antes de usar o Unified Manager.

Estas seções descrevem cada um dos itens mostrados no fluxo de trabalho abaixo.



## Requisitos para instalar o Unified Manager

Antes de iniciar o processo de instalação, verifique se o servidor no qual você deseja instalar o Unified Manager atende aos requisitos específicos de software, hardware, CPU e memória.

O NetApp não oferece suporte a nenhuma modificação do código do aplicativo do Unified Manager. Se você precisar aplicar quaisquer medidas de segurança ao servidor do Unified Manager, faça essas alterações no sistema operacional no qual o Unified Manager está instalado.

Para obter mais detalhes sobre como aplicar medidas de segurança ao servidor do Unified Manager, consulte o artigo da base de dados de Conhecimento.

["Capacidade de suporte para medidas de segurança aplicadas ao Active IQ Unified Manager for Clustered Data ONTAP"](#)

### Informações relacionadas

Para obter mais informações, consulte ["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

## Requisitos de infraestrutura virtual e sistema de hardware

A instalação do Unified Manager em uma infraestrutura virtual ou em um sistema físico deve atender aos requisitos mínimos de memória, CPU e espaço em disco.

A tabela a seguir exibe os valores recomendados para recursos de memória, CPU e espaço em disco. Esses valores foram qualificados para que o Unified Manager atenda aos níveis de desempenho aceitáveis.

Configuração de hardware	Definições recomendadas
RAM	12 GB (requisito mínimo de 8 GB)

Configuração de hardware	Definições recomendadas
Processadores	4 CPUs
Capacidade do ciclo da CPU	Total de 9572 MHz (requisito mínimo de 9572 MHz)
Espaço livre em disco	<ul style="list-style-type: none"> <li>• 5 GB (thin Provisioning)</li> <li>• 152 GB (com provisionamento espesso)</li> </ul>

O Unified Manager pode ser instalado em sistemas com uma pequena quantidade de memória, mas os 12 GB de RAM recomendados garantem que haja memória suficiente disponível para um desempenho ideal e que o sistema possa acomodar clusters e objetos de armazenamento adicionais à medida que sua configuração cresce. Você não deve definir limites de memória na VM em que o Unified Manager é implantado e não deve habilitar recursos (por exemplo, baloneamento) que impeçam o software de utilizar a memória alocada no sistema.

Além disso, há um limite para o número de nós que uma única instância do Unified Manager pode monitorar antes de instalar uma segunda instância do Unified Manager. Para obter mais informações, "[Guia de práticas recomendadas do Unified Manager](#)" consulte .

A troca de páginas de memória afeta negativamente o desempenho do sistema e do aplicativo de gerenciamento. A concorrência por recursos de CPU indisponíveis devido à utilização geral do host pode degradar o desempenho.

### Requisito para uso dedicado

O sistema físico ou virtual no qual você instala o Unified Manager deve ser usado exclusivamente para o Unified Manager e não deve ser compartilhado com outros aplicativos. Outras aplicações podem consumir recursos do sistema e reduzir drasticamente a performance do Unified Manager.

### Requisitos de espaço para backups

Se você planeja usar o recurso de backup e restauração do Unified Manager, atribua capacidade adicional para que o diretório ou disco "data" tenha 150 GB de espaço. Um backup pode ser gravado em um destino local ou em um destino remoto. A prática recomendada é identificar um local remoto externo ao sistema host do Unified Manager que tenha no mínimo 150 GB de espaço.

### Requisitos para conectividade de host

O sistema físico ou o sistema virtual no qual você instala o Unified Manager deve ser configurado de tal forma que você possa obter com êxito `ping` o nome do host a partir do próprio host. No caso da configuração do IPv6, você deve verificar se `ping6` o nome do host é bem-sucedido para garantir que a instalação do Unified Manager seja bem-sucedida.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a IU da Web do produto. Se você configurou um endereço IP estático para a rede durante a implantação, designou um nome para o host de rede. Se você configurou a rede usando DHCP, você deve obter o nome do host do DNS.

Se você pretende permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o nome de domínio totalmente qualificado (FQDN) ou o endereço IP, sua configuração de rede terá que resolver esse nome curto para um FQDN válido.

## Requisitos de software e instalação da VMware

O sistema VMware vSphere no qual você instala o Unified Manager requer versões específicas do sistema operacional e software de suporte.

### Software do sistema operativo

As seguintes versões do VMware ESXi são suportadas:

- ESXi 7,0 e 8,0



O Unified Manager OVA em sistemas VMware vSphere executa o Debian os 11 (bullseye) internamente. Para obter informações sobre as versões do hardware da máquina virtual que as versões suportadas dos servidores ESXi podem suportar, consulte a documentação da VMware.

As seguintes versões do vSphere são suportadas:

- VMware vCenter Server 7,0 e 8,0

Consulte a Matriz de interoperabilidade para obter a lista completa e mais atual de versões ESXi suportadas.

["mysupport.NetApp.com/matrix"](https://mysupport.NetApp.com/matrix)

A hora do servidor VMware ESXi deve ser a mesma que a hora do servidor NTP para que o dispositivo virtual funcione corretamente. A sincronização da hora do servidor VMware ESXi com a hora do servidor NTP impede uma falha de tempo.

### Requisitos de instalação

O VMware High Availability para o dispositivo virtual do Unified Manager é compatível.

Se você implantar um armazenamento de dados NFS em um sistema de storage que esteja executando o software ONTAP, use o plug-in NetApp NFS para VMware VAAI para usar o provisionamento thick.

Se a implantação falhar ao usar seu ambiente habilitado para alta disponibilidade por causa de recursos insuficientes, talvez seja necessário modificar as opções de máquina virtual dos recursos de cluster desativando a prioridade de reinicialização da VM e deixando a resposta de isolamento do host ativada.



Durante a instalação ou atualização do Unified Manager, os patches de segurança e software de terceiros necessários são instalados ou atualizados automaticamente em um sistema VMware vSphere. Como os processos de instalação e atualização do Unified Manager controlam esses componentes, você não deve tentar uma instalação ou atualização independente de qualquer componente de terceiros.

### Navegadores suportados

Para acessar a IU da Web do Unified Manager, use um navegador compatível.

A Matriz de interoperabilidade tem a lista de versões suportadas do navegador.

["mysupport.NetApp.com/matrix"](https://mysupport.NetApp.com/matrix)

Para todos os navegadores, a desativação dos bloqueadores pop-up garante que os recursos do software sejam exibidos corretamente.

Se você planeja configurar o Unified Manager para autenticação SAML, para que um provedor de identidade (IDP) possa autenticar usuários, você deve verificar a lista de navegadores suportados pelo IDP também.

## Requisitos de protocolo e porta

As portas e protocolos necessários permitem a comunicação entre o servidor do Unified Manager e os sistemas de storage gerenciado, servidores e outros componentes.

### Conexões ao servidor do Unified Manager

Em instalações típicas, você não precisa especificar números de porta ao se conectar à IU da Web do Unified Manager, porque as portas padrão são sempre usadas. Por exemplo, como o Unified Manager sempre tenta executar em sua porta padrão, você pode digitar `https://<host>` em vez de `https://<host>:443`.

O servidor do Unified Manager usa protocolos específicos para acessar as seguintes interfaces:

Interface	Protocolo	Porta	Descrição
IU da Web do Unified Manager	HTTP	80	Usado para acessar a IU da Web do Unified Manager; redireciona automaticamente para a porta segura 443.
IU da Web do Unified Manager e programas que usam APIs	HTTPS	443	Usado para acessar com segurança a IU da Web do Unified Manager ou para fazer chamadas de API; as chamadas de API só podem ser feitas usando HTTPS.
Consola de manutenção	SSH/SFTP	22	Usado para acessar o console de manutenção e recuperar pacotes de suporte.
Linha de comando Linux	SSH/SFTP	22	Usado para acessar a linha de comando Red Hat Enterprise Linux e recuperar pacotes de suporte.

Interface	Protocolo	Porta	Descrição
Syslog	UDP	514	Utilizado para aceder a mensagens EMS baseadas em subscrição a partir de sistemas ONTAP e para criar eventos com base nas mensagens.
DESCANSO	HTTPS	9443	Usado para acessar eventos EMS baseados em API REST em tempo real a partir de sistemas ONTAP autenticados.




A porta padrão para MySQL, 3306, é restrita apenas ao localhost durante a instalação do Unified Manager em sistemas VMware vSphere. Isso não afeta nenhum cenário de atualização, onde a configuração anterior é mantida. Esta configuração pode ser modificada e a conexão pode ser disponibilizada a outros hosts usando a `Control access to MySQL port 3306` opção no console de manutenção. Para obter informações, ["Opções de menu adicionais"](#) consulte . As portas usadas para comunicação HTTP e HTTPS (portas 80 e 443) podem ser alteradas usando o console de manutenção do Unified Manager. Para obter mais informações, ["Menus da consola de manutenção"](#) consulte .

### Conexões do servidor do Unified Manager

Você deve configurar seu firewall para abrir portas que habilitem a comunicação entre o servidor do Unified Manager e sistemas de armazenamento gerenciados, servidores e outros componentes. Se uma porta não estiver aberta, a comunicação falhará.

Dependendo do seu ambiente, você pode optar por modificar as portas e protocolos usados pelo servidor do Unified Manager para se conectar a destinos específicos.

O servidor Unified Manager se conecta, usando os seguintes protocolos e portas, aos sistemas de storage gerenciado, servidores e outros componentes:

Destino	Protocolo	Porta	Descrição
Sistema de storage	HTTPS	443/TCP	<p>Usado para monitorar e gerenciar sistemas de storage.</p> <p> Se você estiver usando essa porta ou qualquer outra porta para se conectar ao VMware vCenter Server ou ao servidor ESXi, verifique se a porta está disponível e pode ser conectada em um site seguro.</p>
Sistema de storage	NDMP	10000/TCP	Usado para certas operações de restauração do Snapshot.
Servidor AutoSupport	HTTPS	443	Usado para enviar informações do AutoSupport. Requer o acesso à Internet para executar esta função.
Servidor de autenticação	LDAP	389	Usado para fazer solicitações de autenticação e solicitações de pesquisa de usuários e grupos.
LDAPS	636	Usado para comunicação LDAP segura.	Servidor de correio
SMTP	25	Usado para enviar e-mails de notificação de alerta.	Emissor de trap SNMP



Destino	Protocolo	Porta	Descrição
SNMPv1 ou SNMPv3	162/UDP	Usado para enviar armadilhas SNMP de notificação de alerta.	Servidor de provedor de dados externo
TCP	2003	Usado para enviar dados de desempenho para um provedor de dados externo, como o Graphite.	Servidor NTP

## Completar a folha de trabalho

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

### Informações de instalação do Unified Manager

Os detalhes necessários para instalar o Unified Manager.

Sistema no qual o software é implantado	O seu valor
Endereço IP do servidor ESXi	
Host nome de domínio totalmente qualificado	
Endereço IP do host	
Máscara de rede	
Endereço IP do gateway	
Endereço DNS primário	
Endereço DNS secundário	
Pesquisar domínios	
Nome de utilizador de manutenção	
Palavra-passe do utilizador de manutenção	

### Informações de configuração do Unified Manager


Os detalhes para configurar o Unified Manager após a instalação. Alguns valores são opcionais, dependendo da configuração.

<b>Definição</b>	<b>O seu valor</b>
Endereço de e-mail do usuário de manutenção	
Servidor NTP	
Nome do host do servidor SMTP ou endereço IP	
Nome de utilizador SMTP	
Palavra-passe SMTP	
Porta de SMTP	25 (valor padrão)
E-mail a partir do qual as notificações de alerta são enviadas	
Nome do host ou endereço IP do servidor de autenticação	
Nome de administrador do ativo Directory ou nome distinto de associação LDAP	
Palavra-passe do ativo Directory ou palavra-passe LDAP BIND	
Nome distinto da base do servidor de autenticação	
URL do provedor de identidade (IDP)	
Metadados do provedor de identidade (IDP)	
Endereços IP do host de destino de intercetação SNMP	
Porta de SNMP	

### **Informações do cluster**

Os detalhes dos sistemas de storage que você gerencia usando o Unified Manager.

<b>Cluster 1 de N</b>	<b>O seu valor</b>
Nome do host ou endereço IP de gerenciamento de cluster	

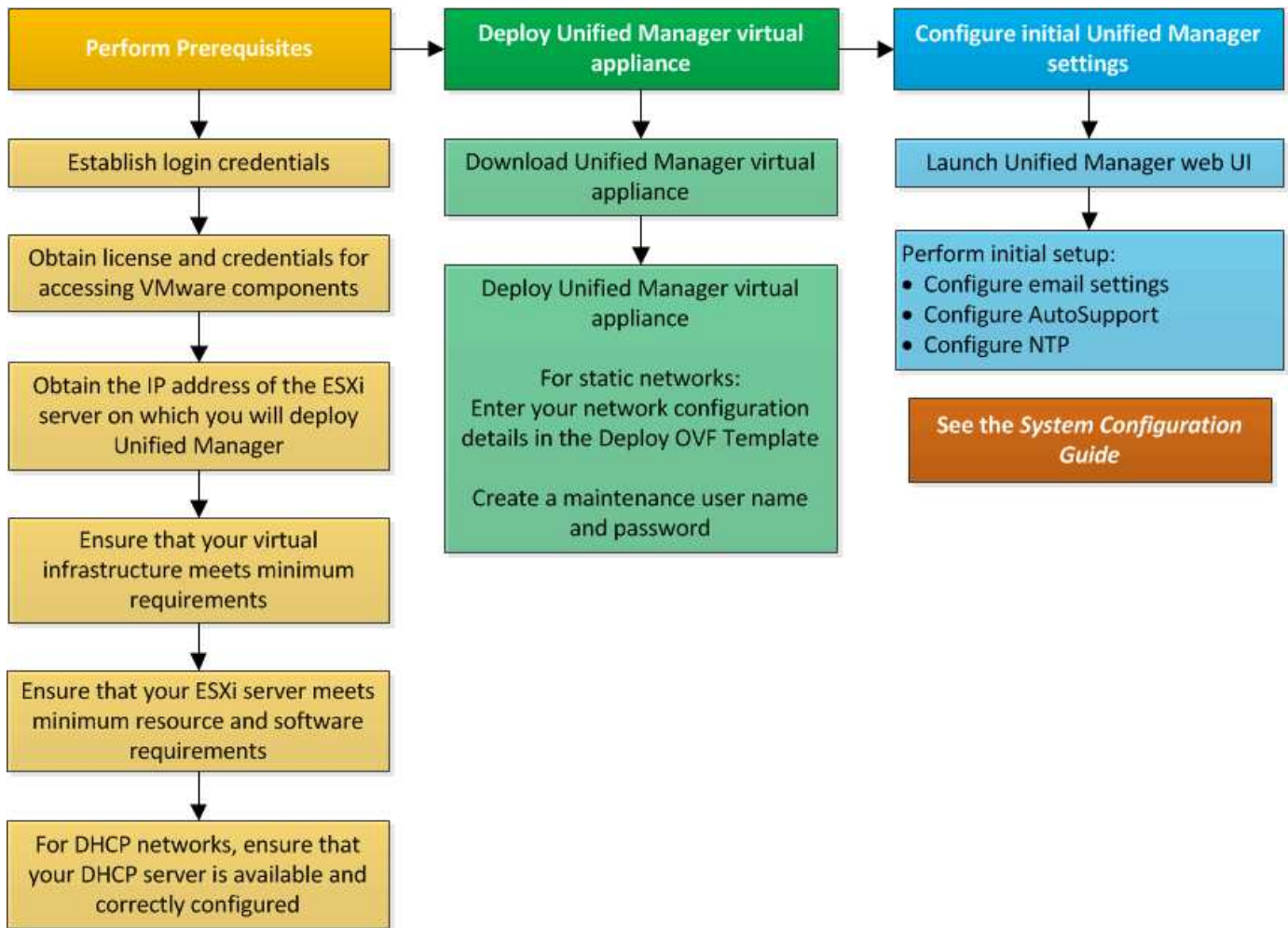
Cluster 1 de N	O seu valor
<p>Nome de usuário do administrador do ONTAP</p> <div data-bbox="167 241 224 300">  </div> <p>O administrador deve ter sido atribuído a função "admin".</p>	
<p>Senha do administrador do ONTAP</p>	
<p>Protocolo</p>	<p>HTTPS</p>

## Instalação, atualização e remoção do software Unified Manager

Nos sistemas VMware vSphere, você pode instalar o Unified Manager, atualizar para uma versão mais recente do software ou remover o vApp (Unified Manager virtual Appliance).

### Visão geral do processo de implantação

O fluxo de trabalho de implantação descreve as tarefas que você deve executar antes de usar o Unified Manager.



## Implantando o Unified Manager

A implantação do Unified Manager inclui o download de software, a implantação do dispositivo virtual, a criação de um nome de usuário e senha de manutenção e a execução da configuração inicial na interface da Web.

### Antes de começar

- Você deve verificar e completar os requisitos do sistema para implantação.

"Requisitos do sistema" Consulte .

- Certifique-se de que tem as seguintes informações:
  - Credenciais de login para o site de suporte da NetApp
  - Credenciais para acessar o VMware vCenter Server e o vSphere Web Client
  - Endereço IP do servidor ESXi no qual você está implantando o dispositivo virtual do Unified Manager
  - Detalhes sobre o data center, como espaço de armazenamento no armazenamento de dados e requisitos de memória
  - IPv6 deve ser ativado no host se você estiver planejando usar endereçamento IPv6.

Você pode implantar o Unified Manager como um dispositivo virtual em um servidor VMware ESXi.

Você deve acessar o console de manutenção usando o console VMware e não usando SSH.



A partir do Unified Manager 9,8, o VMware Tools foi substituído por Open VM Tools (`open-vm-tools`). Você não precisa mais instalar o VMware Tools como parte da instalação porque `open-vm-tools` está incluído no pacote de instalação do Unified Manager.

Depois de concluir a implantação e a configuração inicial, você pode adicionar clusters ou configurar configurações de rede adicionais no console de manutenção e acessar a IU da Web.

### Passos

1. Siga as etapas em "[Faça download do Unified Manager](#)".
2. Além disso, siga as etapas em "[Implante o dispositivo virtual do Unified Manager](#)".

### Download do arquivo de instalação do Unified Manager

Faça download do arquivo de instalação do Unified Manager no site de suporte da NetApp para implantar o Unified Manager como um dispositivo virtual.

#### Antes de começar

Você deve ter as credenciais de login para o site de suporte da NetApp.

O arquivo de instalação é um `.tar` arquivo que contém um certificado raiz, um README arquivo e um OVA arquivo que contém o software Unified Manager configurado para um dispositivo virtual.

### Passos

1. Faça login no site de suporte da NetApp e navegue até a página de download do Gerenciador Unificado: "[Site de suporte da NetApp](#)".
2. Selecione a versão necessária do Unified Manager e aceite o contrato de licença de usuários finais (EULA).
3. Baixe e salve o `.tar` arquivo para instalação do VMware vSphere em um diretório local ou diretório de rede acessível ao cliente vSphere.
4. Verifique a soma de verificação para garantir que o software foi transferido corretamente.
5. Navegue até o diretório em que você baixou o `.tar` arquivo e digite o seguinte comando na janela do terminal para expandir o pacote do Unified Manager:

```
tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz
```

O arquivo necessário OVA, um certificado raiz e um README arquivo para o Unified Manager são descompactados no diretório de destino.

6. Verifique a integridade OVA do arquivo seguindo as etapas fornecidas no README arquivo.

### Implantando o dispositivo virtual do Unified Manager

Depois de fazer o download do arquivo de instalação, você implanta o Unified Manager como um dispositivo virtual. Use o vSphere Web Client para implantar o dispositivo

virtual em um servidor ESXi. Quando você implementa o dispositivo virtual, uma máquina virtual é criada.

### Antes de começar

Deve rever os requisitos do sistema. Faça as alterações necessárias antes de implantar o dispositivo virtual do Unified Manager.

["Requisitos de infraestrutura virtual"](#)Consulte .

["Requisitos de software e instalação da VMware"](#)Consulte .

Se utilizar o DHCP (Dynamic Host Configuration Protocol), certifique-se de que o servidor DHCP está disponível e que as configurações do adaptador de rede DHCP e máquina virtual (VM) estão corretas. O DHCP é configurado por padrão.

Se você usar uma configuração de rede estática, verifique se o endereço IP não está duplicado na mesma sub-rede e se as entradas apropriadas do servidor DNS foram configuradas.

Obtenha as seguintes informações antes de implantar o dispositivo virtual:

- Credenciais para acessar o VMware vCenter Server e o vSphere Web Client
- Endereço IP do servidor ESXi no qual você está implantando o dispositivo virtual do Unified Manager
- Detalhes sobre o data center, como disponibilidade de espaço de storage
- Se você não estiver usando DHCP, obtenha os endereços IPv4 ou IPv6 para os dispositivos de rede aos quais você está planejando se conectar:
  - Nome de domínio totalmente qualificado (FQDN) do host
  - Endereço IP do host
  - Máscara de rede
  - Endereço IP do gateway padrão
  - Endereços DNS primário e secundário
  - Pesquisar domínios

A partir do Unified Manager 9,8, o VMware Tools foi substituído por Open VM Tools *open-vm-tools*). Você não precisa instalar o VMware Tools como parte do processo de instalação porque *open-vm-tools* está incluído no pacote de instalação do Unified Manager.

Quando o dispositivo virtual é implantado, um certificado autoassinado exclusivo para acesso HTTPS é gerado. Ao acessar a IU da Web do Unified Manager, você pode ver um aviso do navegador sobre certificados não confiáveis.

O VMware High Availability para o dispositivo virtual do Unified Manager é compatível.

### Passos

1. No vSphere Client, clique em **File > Deploy OVF Template**.
2. Conclua o assistente implantar modelo OVF para implantar o dispositivo virtual do Unified Manager.

Na página Detalhes da revisão:

- Verifique os detalhes da seção Publisher. A mensagem **Entrust Code Signing - OVCS2 (certificado confiável)** confirma a integridade do arquivo baixado OVA. Se você vir a mensagem **Entrust Code**

**Signing - OVCS2 (Invalid certificate)**, atualize o VMware vCenter Server para a versão 7.0U3E ou superior.

Na página Personalizar modelo:

- Deixe todos os campos em branco ao usar endereçamento DHCP e IPv4.
  - Marque a caixa ""Ativar endereçamento IPv6 automático"" e deixe todos os outros campos em branco ao usar endereçamento DHCP e IPv6.
  - Se você quiser usar uma configuração de rede estática, você pode preencher os campos nesta página e essas configurações serão aplicadas durante a implantação. Certifique-se de que o endereço IP é exclusivo para o host no qual ele é implantado, que ele ainda não está em uso e que ele tem uma entrada DNS válida.
3. Depois que o dispositivo virtual do Unified Manager for implantado no servidor ESXi, ligue a VM clicando com o botão direito do Mouse na VM e, em seguida, selecionando **ligar**.



Se a operação de ativação falhar devido a recursos insuficientes, adicione recursos e tente novamente a instalação.

4. Clique na guia **Console**.

O processo de inicialização inicial leva alguns minutos para ser concluído.

5. Para configurar seu fuso horário, insira sua área geográfica e sua cidade ou região conforme solicitado na janela Console da VM.

Todas as informações de data exibidas usam o fuso horário configurado para o Unified Manager, independentemente da configuração de fuso horário nos dispositivos gerenciados. Se os seus sistemas de armazenamento e o servidor de gestão estiverem configurados com o mesmo servidor NTP, referem-se ao mesmo instante a tempo, mesmo que pareçam diferentes. Por exemplo, se você criar uma cópia Snapshot usando um dispositivo configurado usando um fuso horário diferente do servidor de gerenciamento, o carimbo de hora será a hora do servidor de gerenciamento.

6. Se não houver serviços DHCP disponíveis ou se houver um erro nos detalhes da configuração de rede estática, selecione uma das seguintes opções:

Se você usar...	Então faça isso...
DHCP	<p>Selecione <b>Repetir DHCP</b>. Se pretende utilizar o DHCP, deve certificar-se de que está configurado corretamente.</p> <p>Se você usar uma rede habilitada para DHCP, as entradas do FQDN e do servidor DNS serão dadas automaticamente ao dispositivo virtual. Se o DHCP não estiver configurado corretamente com o DNS, o nome do host ""UnifiedManager"" será atribuído automaticamente e associado ao certificado de segurança. Se não tiver configurado uma rede com DHCP, deverá introduzir manualmente as informações de configuração da rede.</p>

Se você usar...	Então faça isso...
Uma configuração de rede estática	<p>a. Selecione <b>Introduza os detalhes para a configuração de rede estática</b>.</p> <p>O processo de configuração leva alguns minutos para ser concluído.</p> <p>b. Confirme os valores que introduziu e selecione <b>Y</b>.</p>

7. No prompt, insira um nome de usuário de manutenção e clique em **Enter**.

O nome do usuário de manutenção deve começar com uma letra de a-z, seguida de qualquer combinação de -, a-z ou 0-9.

8. No prompt, digite uma senha e clique em **Enter**.

O console da VM exibe o URL da IU da Web do Unified Manager.

Você pode acessar a IU da Web para executar a configuração inicial do Unified Manager, conforme descrito no ["Configurando o Active IQ Unified Manager"](#).

## Atualizando o Unified Manager

Você pode atualizar o Active IQ Unified Manager para a versão 9,16 apenas a partir da versão 9,13 ou 9,14.

Durante o processo de atualização, o Unified Manager não está disponível. Você deve concluir todas as operações em execução antes de atualizar o Unified Manager.

Se o Unified Manager estiver emparelhado com uma instância do OnCommand Workflow Automation e houver novas versões de software disponíveis para ambos os produtos, será necessário desconectar os dois produtos e configurar uma nova conexão do Workflow Automation após a realização das atualizações. Se você estiver executando uma atualização para apenas um dos produtos, deverá fazer login no Workflow Automation após a atualização e verificar se ele ainda está adquirindo dados do Unified Manager.

### Passos

1. Siga as etapas em ["Faça o download da imagem ISO do Unified Manager"](#).
2. Além disso, siga as etapas descritas em ["Atualizar o Unified Manager"](#).

### Caminho de atualização suportado para versões do Unified Manager

O Active IQ Unified Manager suporta um caminho de atualização específico para cada versão.

Nem todas as versões do Unified Manager podem realizar uma atualização no local para versões posteriores. As atualizações do Unified Manager estão limitadas a um modelo N-2, o que significa que uma atualização só pode ser realizada nas próximas versões do 2 em todas as plataformas. Por exemplo, você pode fazer uma atualização para o Unified Manager 9,16 somente do Unified Manager 9,13 e 9,14.

Se você estiver executando uma versão anterior às versões suportadas, sua instância do Unified Manager



precisará ser atualizada primeiro para uma das versões suportadas e, em seguida, atualizada para a versão atual.

Por exemplo, se a versão instalada for o Unified Manager 9,9 e você quiser atualizar para o Unified Manager 9,14, siga uma sequência de atualizações.

#### **Exemplo de caminho de atualização:**

1. Atualização 9,11 → 9,13
2. Atualização 9,13 → 9,14
3. Atualização 9,14 → 9,16

Para obter mais informações sobre a matriz de caminho de atualização, consulte este ["artigo da base de conhecimento \(KB\)"](#).

#### **Download do arquivo de atualização do Unified Manager**

Antes de atualizar o Unified Manager, faça download do arquivo de atualização do Unified Manager no site de suporte da NetApp.

#### **Antes de começar**

Você deve ter credenciais de login para o site de suporte da NetApp.

#### **Passos**

1. Faça login no site de suporte da NetApp:

["Site de suporte da NetApp"](#)

2. Navegue até a página Download para atualizar o Unified Manager no VMware vSphere.
3. Faça o download `.iso` da imagem para atualização e salve-a em um diretório local ou diretório de rede acessível ao seu vSphere Client.
4. Verifique a soma de verificação para garantir que o software foi transferido corretamente.

#### **Atualizando o dispositivo virtual do Unified Manager**

Você pode atualizar o dispositivo virtual Active IQ Unified Manager das versões 9,13 ou 9,14 para 9,16.

#### **Antes de começar**

Certifique-se de que:

- Você baixou o arquivo de atualização, a imagem ISO do site de suporte da NetApp.
- O sistema no qual você está atualizando o Unified Manager atende aos requisitos de sistema e software.

["Requisitos de infraestrutura virtual"](#)Consulte .

["Requisitos de software e instalação da VMware"](#)Consulte .

- Para o vSphere 6,5 e usuários posteriores, você instalou o VMware Remote Console (VMRC).
- Durante a atualização, você pode ser solicitado a confirmar se deseja manter as configurações padrão anteriores para reter dados de desempenho por 13 meses ou alterá-los para 6 meses. Ao confirmar, os

dados históricos de desempenho são purgados após 6 meses.

- Você tem as seguintes informações:
  - Credenciais de login para o site de suporte da NetApp
  - Credenciais para acessar o VMware vCenter Server e o vSphere Web Client
  - Credenciais para o usuário de manutenção do Unified Manager

Durante o processo de atualização, o Unified Manager não está disponível. Você deve concluir todas as operações em execução antes de atualizar o Unified Manager.

Se você emparelhou o Workflow Automation e o Unified Manager, atualize manualmente o nome do host no Workflow Automation.

## Passos

1. No vSphere Client, clique em **Home > Inventory > VMs e modelos**.
2. Selecione a máquina virtual (VM) na qual o dispositivo virtual do Unified Manager está instalado.
3. Se a VM do Unified Manager estiver em execução, navegue até **Summary > Commands > Shut Down Guest**.
4. Crie uma cópia de backup, como um snapshot ou um clone, da VM do Unified Manager para criar um backup consistente com aplicações.
5. A partir do vSphere Client, ligue a VM do Unified Manager.
6. Inicie o VMware Remote Console.
7. Clique no ícone **CDROM** e selecione **Connect to Disk Image File (.iso)**.
8. Selecione o `ActiveIQUnifiedManager-<version>-virtual-update.iso` arquivo e clique em **Open**.
9. Clique na guia **Console**.
10. Faça login no console de manutenção do Unified Manager.
11. No menu principal, selecione **Upgrade**.

É exibida uma mensagem informando que o Unified Manager não estará disponível durante o processo de atualização e será retomado após a conclusão.

12. `y` Digite para continuar.

Um aviso é exibido, lembrando-o de fazer backup da máquina virtual na qual o dispositivo virtual reside.

13. `y` Digite para continuar.

O processo de atualização e a reinicialização dos serviços do Unified Manager podem levar vários minutos para serem concluídos.

14. Prima qualquer tecla para continuar.

Você é desconectado automaticamente do console de manutenção.

15. **Opcional:** Faça login no console de manutenção e verifique a versão do Unified Manager.

Você pode iniciar a IU da Web em uma nova janela em um navegador da Web compatível e fazer login para usar a versão atualizada do Unified Manager. Observe que você precisa esperar que o processo de descoberta termine antes de executar qualquer tarefa na IU.

## Reiniciando a máquina virtual do Unified Manager

É possível reiniciar a máquina virtual (VM) do Unified Manager a partir do console de manutenção. Você deve reiniciar a VM depois de gerar um novo certificado de segurança ou se houver um problema com a VM.

### Antes de começar

- O dispositivo virtual deve ser ligado.
- Você deve estar conectado ao console de manutenção do Unified Manager como usuário de manutenção.

Você também pode reiniciar a máquina virtual do vSphere usando a opção VMware **Restart Guest**.

### Passos

1. No console de manutenção, selecione **Configuração do sistema > Reboot Virtual Machine**.
2. Inicie a IU da Web do Unified Manager a partir do seu navegador e inicie sessão.

### Informações relacionadas

["Referência do VMware vSphere PowerCLI Cmdlets: Restart-VMGuest"](#)

## Remoção do Unified Manager

Você pode desinstalar o Unified Manager removendo a máquina virtual (VM) na qual o software Unified Manager está instalado.

### Antes de começar

- Você deve ter credenciais para acessar o VMware vCenter Server e o vSphere Web Client.
- Qualquer conexão ativa do servidor do Unified Manager a um servidor do Workflow Automation deve ser fechada.
- Todos os clusters (fontes de dados) devem ser removidos do servidor do Unified Manager antes de remover a máquina virtual (VM).

### Passos

1. Use o console de manutenção do Unified Manager para verificar se o servidor do Unified Manager não tem uma conexão ativa com um provedor de dados externo.
2. No vSphere Client, clique em **Home > Inventory > VMs e modelos**.
3. Selecione a VM que você deseja remover e clique na guia **Summary**.
4. Se a VM estiver em execução, clique em **Power > Shut Down Guest**.
5. Clique com o botão direito do rato na VM que pretende remover e clique em **Eliminar do disco**.

# Instale o Unified Manager em sistemas Linux

## Introdução ao Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente chamado Gerenciador Unificado de OnCommand) permite que você monitore e gerencie a integridade e a performance dos sistemas de storage da ONTAP com uma única interface. Você pode implantar o Unified Manager em um servidor Linux, em um servidor Windows ou como um dispositivo virtual (vApp) em um host VMware.

Após concluir a instalação e adicionar os clusters que você deseja gerenciar, o Unified Manager fornece uma interface gráfica que exibe a capacidade, disponibilidade, proteção e status de performance dos sistemas de storage monitorados.

### Informações relacionadas

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

### O que o servidor Unified Manager faz

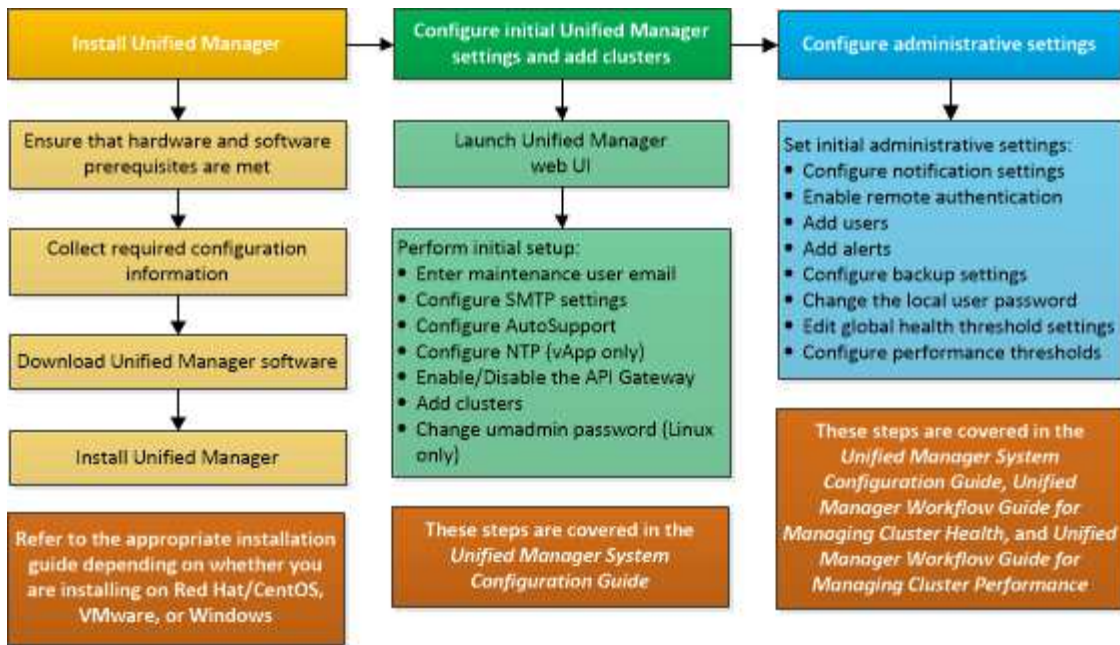
A infraestrutura de servidor do Unified Manager consiste em uma unidade de coleta de dados, um banco de dados e um servidor de aplicativos. Ele fornece serviços de infraestrutura como descoberta, monitoramento, controle de acesso baseado em funções (RBAC), auditoria e logs.

O Unified Manager coleta informações de cluster, armazena os dados no banco de dados e analisa os dados para verificar se há problemas de cluster.

### Descrição geral da sequência de instalação

O fluxo de trabalho de instalação descreve as tarefas que você deve executar antes de usar o Unified Manager.

Estas seções descrevem cada um dos itens mostrados no fluxo de trabalho abaixo.



## Requisitos para instalar o Unified Manager

Antes de iniciar o processo de instalação, verifique se o servidor no qual você deseja instalar o Unified Manager atende aos requisitos específicos de software, hardware, CPU e memória.

O NetApp não oferece suporte a nenhuma modificação do código do aplicativo do Unified Manager. Se você precisar aplicar quaisquer medidas de segurança ao servidor do Unified Manager, faça essas alterações no sistema operacional no qual o Unified Manager está instalado.

Para obter mais detalhes sobre como aplicar medidas de segurança ao servidor do Unified Manager, consulte o artigo da base de dados de Conhecimento.

["Capacidade de suporte para medidas de segurança aplicadas ao Active IQ Unified Manager for Clustered Data ONTAP"](#)

### Informações relacionadas


["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

## Requisitos de infraestrutura virtual e sistema de hardware

A instalação do Unified Manager em uma infraestrutura virtual ou em um sistema físico deve atender aos requisitos mínimos de memória, CPU e espaço em disco.

A tabela a seguir exibe os valores recomendados para recursos de memória, CPU e espaço em disco. Esses valores foram qualificados para que o Unified Manager atenda aos níveis de desempenho aceitáveis.

Configuração de hardware	Definições recomendadas
RAM	12 GB (requisito mínimo de 8 GB)

Configuração de hardware	Definições recomendadas
Processadores	4 CPUs
Capacidade do ciclo da CPU	Total de 9572 MHz (requisito mínimo de 9572 MHz)
Espaço livre em disco	<p>150 GB, onde a capacidade é alocada da seguinte forma:</p> <ul style="list-style-type: none"> <li>• 50 GB atribuídos à partição raiz</li> <li>• 100 GB de espaço livre em disco atribuído ao <code>/opt/netapp/data</code> diretório, que é montado em uma unidade LVM ou em um disco local separado conectado ao sistema de destino</li> </ul> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Para diretórios e <code>/var/log</code> montados separadamente <code>/opt</code>, certifique-se de que <code>/opt</code> tem 15 GB e <code>/var/log</code> tem 16 GB de espaço livre. O <code>/tmp</code> diretório deve ter pelo menos 10 GB de espaço livre.</p> </div>

O Unified Manager pode ser instalado em sistemas com uma pequena quantidade de memória, mas os 12 GB de RAM recomendados garantem que haja memória suficiente disponível para um desempenho ideal e que o sistema possa acomodar clusters e objetos de armazenamento adicionais à medida que sua configuração cresce. Você não deve definir limites de memória na VM em que o Unified Manager é implantado e não deve habilitar recursos (por exemplo, baloneamento) que impeçam o software de utilizar a memória alocada no sistema.

Além disso, há um limite para o número de nós que uma única instância do Unified Manager pode monitorar antes de instalar uma segunda instância do Unified Manager. Para obter mais informações, consulte o *Guia de práticas recomendadas*.

["Relatório técnico 4621: Guia de práticas recomendadas do Unified Manager"](#)

A troca de páginas de memória afeta negativamente o desempenho do sistema e do aplicativo de gerenciamento. A concorrência por recursos de CPU indisponíveis devido à utilização geral do host pode degradar o desempenho.

### Requisito para uso dedicado

O sistema físico ou virtual no qual você instala o Unified Manager deve ser usado exclusivamente para o Unified Manager e não deve ser compartilhado com outros aplicativos. Outras aplicações podem consumir recursos do sistema e reduzir drasticamente a performance do Unified Manager.

### Requisitos de espaço para backups

Se você planeja usar o recurso de backup e restauração do Unified Manager, atribua capacidade adicional para que o diretório ou disco "data" tenha 150 GB de espaço. Um backup pode ser gravado em um destino local ou em um destino remoto. A prática recomendada é identificar um local remoto externo ao sistema host do Unified Manager que tenha no mínimo 150 GB de espaço.

## Requisitos para conectividade de host

O sistema físico ou o sistema virtual no qual você instala o Unified Manager deve ser configurado de tal forma que você possa obter com êxito `ping` o nome do host a partir do próprio host. No caso da configuração do IPv6, você deve verificar se `ping6` o nome do host é bem-sucedido para garantir que a instalação do Unified Manager seja bem-sucedida.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a IU da Web do produto. Se você configurou um endereço IP estático para a rede durante a implantação, designou um nome para o host de rede. Se você configurou a rede usando DHCP, você deve obter o nome do host do DNS.

Se você pretende permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o nome de domínio totalmente qualificado (FQDN) ou o endereço IP, sua configuração de rede terá que resolver esse nome curto para um FQDN válido.

## Requisitos de software e instalação do Linux

O sistema Linux no qual você instala o Unified Manager requer versões específicas do sistema operacional e software de suporte.

### Software do sistema operativo

O sistema Linux deve ter as seguintes versões do sistema operacional e o software de suporte instalado:

- Red Hat Enterprise Linux versões 8.x e 9.4, com base na arquitetura x86\_64.

Consulte a Matriz de interoperabilidade para obter a lista completa e mais atual das versões Linux suportadas do Red Hat Enterprise.

["mysupport.NetApp.com/matrix"](https://mysupport.netapp.com/matrix)

O servidor deve ser dedicado à execução do Unified Manager. Nenhum outro aplicativo deve ser instalado no servidor. É possível que o scanner de vulnerabilidade como o Qualys esteja instalado em seu sistema Linux por causa dos regulamentos da empresa. Você deve desativar o scanner de vulnerabilidades antes de instalar o Unified Manager para evitar que a instalação falhe.



Os scanners de vulnerabilidade (como Qualys) podem levar ao alto uso da CPU ao digitalizar a máquina virtual (VM) internamente (onde o Unified Manager e o verificador de vulnerabilidades estão instalados na mesma VM) ou externamente (onde o Unified Manager e o verificador de vulnerabilidades estão instalados em dois servidores diferentes e o verificador de vulnerabilidade verifica a VM onde o Unified Manager está instalado). Esse problema geralmente faz com que a VM não responda e afete os serviços do Unified Manager. Portanto, o NetApp recomenda desativar o scanner de vulnerabilidades na VM onde o Gerenciador Unificado está instalado. Se a desativação do scanner não for uma opção, digitalize a VM durante o horário comercial e reinicie os serviços após a conclusão da digitalização.

### Software de terceiros

O Unified Manager é implantado em um servidor web WildFly. O WildFly 26.1.3 é empacotado e configurado com o Unified Manager.

Os seguintes pacotes de terceiros são necessários, mas não estão incluídos no Unified Manager. Esses pacotes são instalados automaticamente pelo `yum` instalador durante a instalação, desde que você tenha configurado os repositórios como mencionado nas seções a seguir.

- MySQL Community Edition versão 8.0.37 (do repositório MySQL).
- OpenJDK versão 11.0.23 (do repositório Red Hat extra Enterprise Linux Server)
- Python 3,9.x (do repositório do Red Hat extra Enterprise Linux Server)
- p7zip versão 16,02 ou posterior (a partir do repositório Red Hat extra Packages for Enterprise Linux)



Você deve encerrar uma instância em execução do Unified Manager antes de atualizar qualquer software de terceiros. Depois que a instalação de software de terceiros estiver concluída, você poderá reiniciar o Unified Manager.

## Requisitos de autorização do utilizador

A instalação do Unified Manager em um sistema Linux pode ser realizada pelo usuário raiz ou por usuários não-root usando o `sudo` comando.

## Requisitos de instalação

As melhores práticas para instalar o Red Hat Enterprise Linux e os repositórios associados em seu sistema estão listadas abaixo. Os sistemas instalados ou configurados de forma diferente ou implantados fora do local (na nuvem) podem exigir etapas adicionais, e o Unified Manager pode não ser executado corretamente em tais implantações.

- Você deve instalar o Red Hat Enterprise Linux de acordo com as melhores práticas da Red Hat, e você deve selecionar as seguintes opções padrão, o que requer a seleção do ambiente base "Server with GUI".
- Ao instalar o Unified Manager no Red Hat Enterprise Linux, o sistema precisa ter acesso ao repositório apropriado para que o programa de instalação possa acessar e instalar todas as dependências de software necessárias.
- Para que o `yum` instalador encontre software dependente nos repositórios Red Hat Enterprise Linux, você deve ter registrado o sistema durante a instalação do Red Hat Enterprise Linux ou depois usando uma assinatura válida do Red Hat.

Consulte a documentação da Red Hat para obter informações sobre o Red Hat Subscription Manager.

- Você deve habilitar o repositório Pacotes extras para o Enterprise Linux (EPEL) para instalar com êxito os utilitários de terceiros necessários no seu sistema.

Se o repositório EPEL não estiver configurado no sistema, você deverá baixar e configurar manualmente o repositório.

["Configurando manualmente o repositório EPEL"](#) Consulte .

- Se a versão correta do MySQL não estiver instalada, você deve habilitar o repositório MySQL para instalar com sucesso o software MySQL em seu sistema.

Se o repositório MySQL não estiver configurado em seu sistema, você deverá baixar e configurar manualmente o repositório.

["Configurando manualmente o repositório MySQL"](#) Consulte .

Se o seu sistema não tiver acesso à Internet e os repositórios não forem espelhados de um sistema ligado à Internet para o sistema não ligado, siga as instruções de instalação para determinar as dependências de



software externas do seu sistema. Em seguida, pode transferir o software necessário para o sistema ligado à Internet e copiar os `.rpm` ficheiros para o sistema no qual pretende instalar o Unified Manager. Para baixar os artefactos e pacotes, você deve usar o `yum install` comando. Você deve garantir que os dois sistemas estejam executando a mesma versão do sistema operacional e que a licença de assinatura seja para o Red Hat Enterprise Linux apropriado.



Você não deve instalar o software de terceiros necessário de repositórios que não sejam os repositórios listados aqui. O software instalado a partir dos repositórios Red Hat foi projetado explicitamente para o Red Hat Enterprise Linux e está em conformidade com as práticas recomendadas da Red Hat (layouts de diretório, permissões e assim por diante). O software de outros locais pode não seguir essas diretrizes, o que pode causar falha na instalação do Unified Manager ou causar problemas com atualizações futuras.

### Requisito da porta 443

As imagens genéricas do Red Hat Enterprise Linux podem bloquear o acesso externo à porta 443. Devido a essa restrição, talvez você não consiga se conectar à IU da Web do Administrador depois de instalar o Unified Manager. Executar o seguinte comando permite o acesso à porta 443 para todos os usuários e aplicativos externos em um Red Hat Enterprise Linux genérico.

```
# firewall-cmd --zone=public --add-port=443/tcp --permanent; firewall-cmd --reload
```

Você deve instalar o Red Hat Enterprise Linux com o ambiente base "Server with GUI". Ele fornece os comandos usados pelas instruções de instalação do Unified Manager. Outros ambientes básicos podem exigir a instalação de comandos adicionais para validar ou concluir a instalação. Se o `firewall-cmd` não estiver disponível no sistema, você deverá instalá-lo executando o seguinte comando:

```
# sudo yum install firewalld
```

Contacte o departamento DE TI antes de executar os comandos para ver se as suas políticas de segurança requerem um procedimento diferente.



O THP (páginas enormes transparentes) deve ser desativado nos sistemas Red Hat. Quando ativado, em alguns casos, ele pode fazer com que o Unified Manager seja desligado quando certos processos consomem muita memória e são encerrados.

### Navegadores suportados

Para acessar a IU da Web do Unified Manager, use um navegador compatível.

A Matriz de interoperabilidade tem a lista de versões suportadas do navegador.

["mysupport.NetApp.com/matrix"](https://my.support.netapp.com/matrix)

Para todos os navegadores, a desativação dos bloqueadores pop-up garante que os recursos do software sejam exibidos corretamente.

Se você planeja configurar o Unified Manager para autenticação SAML, para que um provedor de identidade (IDP) possa autenticar usuários, você deve verificar a lista de navegadores suportados pelo IDP também.

## Requisitos de protocolo e porta

As portas e protocolos necessários permitem a comunicação entre o servidor do Unified Manager e os sistemas de storage gerenciado, servidores e outros componentes.

### Conexões ao servidor do Unified Manager

Em instalações típicas, você não precisa especificar números de porta ao se conectar à IU da Web do Unified Manager, porque as portas padrão são sempre usadas. Por exemplo, como o Unified Manager sempre tenta executar em sua porta padrão, você pode digitar `https://<host>` em vez de `https://<host>:443`.

O servidor do Unified Manager usa protocolos específicos para acessar as seguintes interfaces:

Interface	Protocolo	Porta	Descrição
IU da Web do Unified Manager	HTTP	80	Usado para acessar a IU da Web do Unified Manager; redireciona automaticamente para a porta segura 443.
IU da Web do Unified Manager e programas que usam APIs	HTTPS	443	Usado para acessar com segurança a IU da Web do Unified Manager ou para fazer chamadas de API; as chamadas de API só podem ser feitas usando HTTPS.
Consola de manutenção	SSH/SFTP	22	Usado para acessar o console de manutenção e recuperar pacotes de suporte.
Linha de comando Linux	SSH/SFTP	22	Usado para acessar a linha de comando Red Hat Enterprise Linux e recuperar pacotes de suporte.
Banco de dados MySQL	MySQL	3306	Usado para habilitar o acesso aos Serviços de API do OnCommand Workflow Automation e do OnCommand ao Unified Manager.

Interface	Protocolo	Porta	Descrição
Syslog	UDP	514	Utilizado para acessar a mensagens EMS baseadas em subscrição a partir de sistemas ONTAP e para criar eventos com base nas mensagens.
DESCANSO	HTTPS	9443	Usado para acessar eventos EMS baseados em API REST em tempo real a partir de sistemas ONTAP autenticados.



A porta padrão para MySQL, 3306, é restrita apenas ao localhost durante a instalação do Unified Manager em sistemas Linux. Isso não afeta nenhum cenário de atualização, onde a configuração anterior é mantida. Esta configuração pode ser modificada e a conexão pode ser disponibilizada a outros hosts usando a `Control access to MySQL port 3306` opção no console de manutenção. Para obter informações, ["Opções de menu adicionais"](#) consulte . As portas usadas para comunicação HTTP e HTTPS (portas 80 e 443) podem ser alteradas usando o console de manutenção do Unified Manager. Para obter mais informações, ["Menus da consola de manutenção"](#) consulte .

### Conexões do servidor do Unified Manager

Você deve configurar seu firewall para abrir portas que habilitem a comunicação entre o servidor do Unified Manager e sistemas de armazenamento gerenciados, servidores e outros componentes. Se uma porta não estiver aberta, a comunicação falhará.

Dependendo do seu ambiente, você pode optar por modificar as portas e protocolos usados pelo servidor do Unified Manager para se conectar a destinos específicos.

O servidor Unified Manager se conecta, usando os seguintes protocolos e portas, aos sistemas de storage gerenciado, servidores e outros componentes:

Destino	Protocolo	Porta	Descrição
Sistema de storage	HTTPS	443/TCP	Usado para monitorar e gerenciar sistemas de storage.
Sistema de storage	NDMP	10000/TCP	Usado para certas operações de restauração do Snapshot.

Destino	Protocolo	Porta	Descrição
Servidor AutoSupport	HTTPS	443	Usado para enviar informações do AutoSupport. Requer o acesso à Internet para executar esta função.
Servidor de autenticação	LDAP	389	Usado para fazer solicitações de autenticação e solicitações de pesquisa de usuários e grupos.
LDAPS	636	Usado para comunicação LDAP segura.	Servidor de correio
SMTP	25	Usado para enviar e-mails de notificação de alerta.	Emissor de trap SNMP
SNMPv1 ou SNMPv3	162/UDP	Usado para enviar armadilhas SNMP de notificação de alerta.	Servidor de provedor de dados externo
TCP	2003	Usado para enviar dados de desempenho para um provedor de dados externo, como o Graphite.	Servidor NTP

## Completar a folha de trabalho

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

### Informações de instalação do Unified Manager

Os detalhes necessários para instalar o Unified Manager.

Sistema no qual o software é implantado	O seu valor
Host nome de domínio totalmente qualificado	
Endereço IP do host	
Máscara de rede	
Endereço IP do gateway	

<b>Sistema no qual o software é implantado</b>	<b>O seu valor</b>
Endereço DNS primário	
Endereço DNS secundário	
Pesquisar domínios	
Nome de utilizador de manutenção	
Palavra-passe do utilizador de manutenção	

### **Informações de configuração do Unified Manager**


Os detalhes para configurar o Unified Manager após a instalação. Alguns valores são opcionais, dependendo da configuração.

<b>Definição</b>	<b>O seu valor</b>
Endereço de e-mail do usuário de manutenção	
Nome do host do servidor SMTP ou endereço IP	
Nome de utilizador SMTP	
Palavra-passe SMTP	
Porta de SMTP	25 (valor padrão)
E-mail a partir do qual as notificações de alerta são enviadas	
Nome do host ou endereço IP do servidor de autenticação	
Nome de administrador do active Directory ou nome distinto de associação LDAP	
Palavra-passe do active Directory ou palavra-passe LDAP BIND	
Nome distinto da base do servidor de autenticação	
URL do provedor de identidade (IDP)	
Metadados do provedor de identidade (IDP)	

Definição	O seu valor
Endereços IP do host de destino de intercetação SNMP	
Porta de SNMP	

### Informações do cluster

Os detalhes dos sistemas de storage que você gerencia usando o Unified Manager.

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

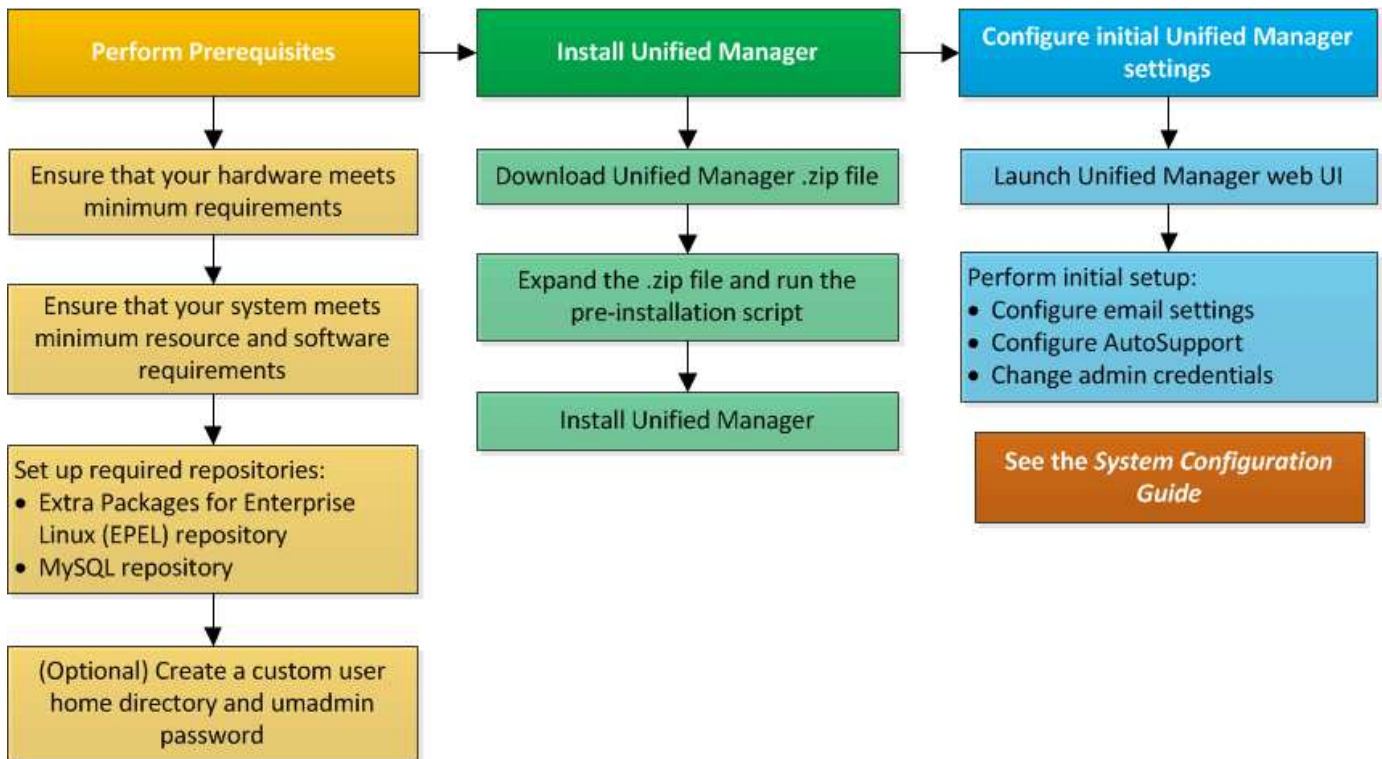
## Instalação, atualização e remoção do software Unified Manager

Em sistemas Linux, você pode instalar o software Unified Manager, atualizar para uma versão mais recente do software ou remover o Unified Manager.

O Unified Manager pode ser instalado em servidores Red Hat Enterprise Linux. O servidor Linux no qual você instala o Unified Manager pode ser executado em uma máquina física ou em uma máquina virtual em execução no VMware ESXi, Microsoft Hyper-V ou Citrix XenServer.

### Visão geral do processo de instalação

O fluxo de trabalho de instalação descreve as tarefas que você deve executar antes de usar o Unified Manager.



## Configurando repositórios de software necessários

O sistema deve ter acesso a determinados repositórios para que o programa de instalação possa acessar e instalar todas as dependências de software necessárias.

### Configurando manualmente o repositório EPEL

Se o sistema no qual você está instalando o Unified Manager não tiver acesso ao repositório Pacotes extras para o Enterprise Linux (EPEL), então você deverá baixar e configurar manualmente o repositório para uma instalação bem-sucedida.

O repositório EPEL fornece acesso aos utilitários de terceiros necessários que devem ser instalados no seu sistema. Você usa o repositório EPEL para instalar o Unified Manager em um sistema Red Hat Enterprise Linux.

#### Passos

1. Baixe o repositório EPEL para sua instalação. Para a versão 8, faça o download em:

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

Para a versão 9, faça o download em:

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

2. Configure o repositório EPEL:

```
yum install epel-release-latest-<version>.noarch.rpm
```

Para sistemas Red Hat Enterprise Linux 8, se você tiver repositórios internos com pacotes RPM modulares,

por exemplo `javapackages-filesystem-<version>.module.rpm`, certifique-se de que os metadados para os pacotes modulares também estejam disponíveis no mesmo repositório.

## Configurando manualmente o repositório MySQL

Se o sistema no qual você está instalando o Unified Manager não tiver acesso ao repositório do MySQL Community Edition, você deverá baixar e configurar manualmente o repositório para uma instalação bem-sucedida.

O repositório MySQL fornece acesso ao software MySQL necessário que deve ser instalado em seu sistema.



Esta tarefa poderá falhar se o sistema não tiver a ligação à Internet. Consulte a documentação do MySQL se o sistema no qual você está instalando o Unified Manager não tiver acesso à Internet.

### Passos

1. Baixe o repositório MySQL apropriado para sua instalação. Para a versão 8, faça o download em:

```
wget http://repo.mysql.com/yum/mysql-8.0-community/el/8/x86_64/mysql80-community-release-el8-1.noarch.rpm
```

Para a versão 9, faça o download em:

```
wget http://repo.mysql.com/yum/mysql-8.0-community/el/9/x86_64/mysql80-community-release-el9-1.noarch.rpm
```

2. Configure o repositório MySQL:

```
yum install mysql80-community-release-<version>.noarch.rpm
```

Para o sistema Red Hat Enterprise Linux 8, se você tiver repositórios internos com `java-11-openjdk`, `p7zip` e outros pacotes de software fornecidos pelo repositório AppStream, você deverá desativar o repositório AppStream e instalar o MySQL Community Server. Execute o seguinte comando:

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install mysql-community-server
```

Se você receber um erro na falta de correspondência de chave ou chave e a instalação falhar, tente estas etapas:

- Em um sistema conectado, importe a chave MySQL atualizada executando o seguinte comando:

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-<xxxx>  
  
for example:  
  
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022
```



- Em um sistema que não tenha conectividade com a Internet, atualize seu arquivo de repositório MySQL e desative `gpgcheck` marcando `gpgcheck=0`.

## Requisitos de SELinux em compartilhamentos NFS e CIFS

Se você está planejando montar `/opt/netapp` ou `/opt/netapp/data` em um dispositivo nas ou SAN e tem o SELinux habilitado, você precisa estar ciente de algumas considerações.

Se você está planejando montar `/opt/netapp` ou `/opt/netapp/data` de qualquer lugar que não seja o sistema de arquivos raiz, e você tem o SELinux habilitado em seu ambiente, você deve definir o contexto correto para os diretórios montados. Para o cenário aplicável em seu ambiente, siga estas etapas para configurar e confirmar o contexto correto do SELinux.

### Configurando o contexto SELinux `/opt/netapp/data` quando estiver montado

Se você tiver montado `/opt/netapp/data` no sistema e o SELinux estiver definido como `Enforcing`, certifique-se de que o tipo de contexto SELinux for `/opt/netapp/data` definido como `mysqld_db_t`, que é o elemento de contexto padrão para a localização dos arquivos do banco de dados.

1. Execute este comando para verificar o contexto:

```
ls -dZ /opt/netapp/data
```

Uma saída de amostra:

```
drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0
/opt/netapp/data
```



Nesta saída, o contexto é `default_t`. Você deve alterar esse contexto para `mysqld_db_t`.

2. Execute estas etapas para definir o contexto com base em como você montou `/opt/netapp/data`.

- a. Execute os seguintes comandos para definir o contexto como `mysqld_db_t`:

```
semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"
`restorecon -R -v /opt/netapp/data
```

- b. Se tiver configurado `/opt/netapp/data` no `/etc/fstab`, deverá editar o `/etc/fstab` arquivo. Para a `/opt/netapp/data/` opção de montagem, adicione o rótulo MySQL como:

```
context=system_u:object_r:mysqld_db_t:s0
```

- c. Desmonte e remonte `/opt/netapp/data/` para ativar o contexto.

- d. Se você tiver uma montagem NFS direta, execute o seguinte comando para definir o contexto como `mysqld_db_t`:

```
mount <nfsshare>:<mountpoint> /opt/netapp/data -o
context=system_u:object_r:mysqld_db_t:s0
```

3. Verifique se o contexto está definido corretamente:

```
ls -dZ /opt/netapp/data/
```

Uma saída de amostra:

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysql_db_t:s0
/opt/netapp/data/
```

### **Configurando o contexto SELinux /opt/netapp quando montado, e /opt/netapp/data/ também é montado separadamente**

Neste cenário, no início, você deve definir o contexto /opt/netapp/data/ como descrito na seção anterior. Depois de definir o contexto correto para /opt/netapp/data/, certifique-se de que o diretório pai /opt/netapp não tem o contexto SELinux definido como file\_t.

#### **Passos**

1. Execute este comando para verificar o contexto:

```
ls -dZ /opt/netapp
```

Uma saída de amostra:

```
drwxr-xr-x. mysql root unconfined_u:object_r:file_t:s0 /opt/netapp
```

Nesta saída, o contexto é file\_t deve ser alterado. Os comandos a seguir definem o contexto como usr\_t. Você pode definir o contexto para qualquer valor que não seja file\_t com base em seus requisitos de segurança.

2. Execute estas etapas para definir o contexto, com base em como você montou /opt/netapp`o .

a. Execute os seguintes comandos para definir o contexto:

```
semanage fcontext -a -t usr_t "/opt/netapp"
restorecon -v /opt/netapp
```

1. Se tiver configurado /opt/netapp no /etc/fstab, deverá editar o /etc/fstab ficheiro. Para a /opt/netapp opção de montagem, adicione o rótulo MySQL como:

```
context=system_u:object_r:usr_t:s0
```

2. Desmonte e, em seguida, monte novamente /opt/netapp para ativar o contexto.

3. Se você tiver uma montagem NFS direta, execute o seguinte comando para definir o contexto:

```
mount <nfsshare>:/<mountpoint> /opt/netapp -o
context=system_u:object_r:usr_t:s0
```

a. Verifique se o contexto está definido corretamente:

```
ls -dZ /opt/netapp
```

Uma saída de amostra

```
drwxr-xr-x. mysql root unconfined_u:object_r:usr_t:s0 /opt/netapp
```

### Configurando o contexto SELinux /opt/netapp quando o é montado e /opt/netapp/data/ não é montado separadamente

Se você tiver montado /opt/netapp no sistema e o SELinux estiver definido como Enforcing, certifique-se de que o tipo de contexto SELinux for /opt/netapp definido como `mysqld_db_t`, que é o elemento de contexto padrão para a localização dos arquivos do banco de dados.

#### Passos

1. Execute este comando para verificar o contexto:

```
ls -dZ /opt/netapp
```

Uma saída de amostra:

```
drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0 /opt/netapp
```



Nesta saída, o contexto é `default_t`. Você deve alterar esse contexto para `mysqld_db_t`.

2. Execute as etapas a seguir para definir o contexto com base em como você montou /opt/netapp.
  - a. Execute os seguintes comandos para definir o contexto como `mysqld_db_t`:

```
semanage fcontext -a -t mysqld_db_t "/opt/netapp"  
`restorecon -R -v /opt/netapp
```
  - b. Se tiver configurado /opt/netapp no /etc/fstab, edite o /etc/fstab arquivo. Para a /opt/netapp/ opção de montagem, adicione o rótulo MySQL como:

```
context=system_u:object_r:mysqld_db_t:s0
```
  - c. Desmonte e, em seguida, monte novamente /opt/netapp/ para ativar o contexto.
  - d. Se você tiver uma montagem NFS direta, execute o seguinte comando para definir o contexto como `mysqld_db_t`:

```
mount <nfsshare>:/<mountpoint> /opt/netapp -o  
context=system_u:object_r:mysqld_db_t:s0
```

3. Verifique se o contexto está definido corretamente:

```
ls -dZ /opt/netapp/
```

Uma saída de amostra:

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysqld_db_t:s0 /opt/netapp/
```

---

## Instalar o Unified Manager em sistemas Linux

É importante que você entenda que a sequência de etapas para baixar e instalar o Unified Manager varia de acordo com o cenário de instalação.

### Criando um diretório inicial personalizado do usuário e uma senha umadmin antes da instalação

Você pode criar um diretório inicial personalizado e definir sua própria senha de usuário umadmin antes de instalar o Unified Manager. Essa tarefa é opcional, mas alguns sites podem precisar de flexibilidade para substituir as configurações padrão de instalação do Unified Manager.

#### Antes de começar

- O sistema deve satisfazer os requisitos descritos na "[Requisitos do sistema de hardware](#)".
- Você deve ser capaz de fazer login como usuário raiz no sistema Red Hat Enterprise Linux.

A instalação padrão do Unified Manager executa as seguintes tarefas:

- Cria o usuário umadmin com `/home/umadmin` como diretório home.
- Atribui a senha padrão "admin" ao usuário umadmin.

Como alguns ambientes de instalação restringem o acesso `/home` ao `root`, a instalação falha. Você deve criar o diretório home em um local diferente. Além disso, alguns sites podem ter regras sobre complexidade de senha ou exigir que as senhas sejam definidas por administradores locais, em vez de serem definidas pelo programa de instalação.

Se o ambiente de instalação exigir que você substitua essas configurações padrão de instalação, siga estas etapas para criar um diretório inicial personalizado e definir a senha do usuário umadmin.

Quando essas informações são definidas antes da instalação, o script de instalação descobre essas configurações e usa os valores definidos em vez de usar as configurações padrão de instalação.

Além disso, a instalação padrão do Unified Manager inclui o usuário umadmin nos arquivos sudoers (`ocum_sudoers`e `ocie_sudoers`) no `/etc/sudoers.d/` diretório. Se você remover esse conteúdo do seu ambiente por causa de políticas de segurança ou por causa de alguma ferramenta de monitoramento de segurança, será necessário adicioná-lo de volta. Você precisa preservar a configuração dos sudoers porque algumas operações do Unified Manager exigem esses sudo Privileges.

As políticas de segurança no seu ambiente não devem restringir o sudo Privileges para o usuário de manutenção do Unified Manager. Algumas operações do Unified Manager podem falhar se o Privileges for restrito. Verifique se você é capaz de executar o seguinte comando sudo quando conectado como o usuário umadmin após a instalação bem-sucedida.

```
sudo systemctl status ocie
```

Este comando deve retornar o status apropriado do serviço ocie sem erros.

#### Passos

1. Inicie sessão como utilizador raiz no servidor.
2. Crie a conta do grupo umadmin chamada "mainblance":

```
groupadd maintenance
```

3. Crie a conta de usuário "umadmin" no grupo de manutenção sob um diretório de sua escolha:

```
adduser --home <home_directory> -g maintenance umadmin
```

4. Defina a senha umadmin:

```
passwd umadmin
```

O sistema solicita que você insira uma nova string de senha para o usuário umadmin.

Depois de instalar o Unified Manager, você deve especificar o shell de login do usuário umadmin.

## A transferir o Unified Manager

Você deve fazer download do arquivo do Gerenciador Unificado .zip no site de suporte da NetApp para instalar o Gerenciador unificado.

### Antes de começar

Você deve ter credenciais de login para o site de suporte da NetApp.

Você faz o download do pacote de instalação do Unified Manager para o sistema Red Hat Enterprise Linux.

### Passos

1. Faça login no site de suporte da NetApp e navegue até a página de download do Gerenciador Unificado:

["Site de suporte da NetApp"](#)

2. Selecione a versão necessária do Unified Manager e aceite o contrato de licença de usuários finais (EULA).
3. Faça o download do arquivo do instalador do Unified Manager para Linux e salve o .zip arquivo em um diretório no sistema de destino.



- Certifique-se de baixar a versão correta do arquivo de instalação para o seu sistema Red Hat Enterprise Linux. Com base se você tem o Red Hat Enterprise Linux 8 ou 9 instalado, certifique-se de baixar a versão apropriada do arquivo Unified Manager .zip.
- A NetApp recomenda que você baixe o certificado de assinatura de código (.pem) e a assinatura digital (.sig) junto com o .zip arquivo.

4. Verifique a integridade do software transferido na soma de verificação.
5. Se você tiver baixado o certificado de assinatura de código e a assinatura digital, poderá verificar a integridade do arquivo do instalador. Você pode usar os seguintes comandos para verificar a integridade do arquivo do instalador:
  - Este comando cria um arquivo com a chave pública a partir do certificado de assinatura de código:

```
openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem >  
<public_key_file_name>
```

- Onde **AIQUM-RHEL-CLIENT-INTER-ROOT.pem** é o arquivo que contém o certificado de assinatura de código.
- Este comando verifica a assinatura no arquivo do instalador:

```
openssl dgst -sha256 -verify <public_key_file_name> -signature
<signature_file_name> ActiveIQUnifiedManager-<version>.zip
```

A mensagem semelhante a `Verified Ok` confirma que o arquivo do instalador é seguro de usar.

## Instalar o Unified Manager

Você pode instalar o Unified Manager em uma plataforma virtual ou física do Red Hat Enterprise Linux.

### Antes de começar

- O sistema no qual você deseja instalar o Unified Manager deve atender aos requisitos de sistema e software.

["Requisitos do sistema de hardware"](#) Consulte .

["Requisitos de software e instalação do Linux"](#) Consulte .

- Você deve ter baixado o arquivo do Gerenciador Unificado .zip do site de suporte da NetApp para o sistema de destino.
- Você deve ter verificado a integridade do arquivo baixado .zip.
- Você deve ter um navegador da Web compatível.
- O software de emulação de terminal deve ter o scrollback habilitado.

O sistema Red Hat Enterprise Linux pode ter todas as versões necessárias do software de suporte necessário (Java, MySQL, utilitários adicionais) instalado, apenas alguns dos softwares necessários instalados ou pode ser um sistema recém-instalado sem nenhum dos softwares necessários instalados.

### Passos

1. Faça login no servidor no qual você está instalando o Unified Manager.
2. Digite os comandos apropriados para avaliar qual software pode exigir instalação ou atualização no sistema de destino para suportar a instalação:

Software necessário e versão mínima	Comando para verificar o software e a versão
OpenJDK versão 11.0.23	<code>java -version</code>
MySQL 8.0.37 Community Edition	<code>`rpm -qa</code>
<code>grep -i mysql`</code>	<code>p7zip 16,02</code>
<code>`rpm -qa</code>	<code>grep p7zip`</code>

3. Se a versão instalada do MySQL for anterior ao MySQL 8.0.37 Community Edition, digite o seguinte comando para desinstalá-lo:

```
rpm -e <mysql_package_name>
```

Se você receber erros de dependência, você deve adicionar a `--nodeps` opção para desinstalar o componente.

4. Navegue até o diretório em que você baixou o arquivo de instalação `.zip` e expanda o pacote do Unified Manager:

```
unzip ActiveIQUnifiedManager-<version>.zip
```

Os `.rpm` módulos necessários para o Unified Manager são descompactados para o diretório de destino.

5. Verifique se o seguinte módulo está disponível no diretório:

```
ls *.rpm
```

```
netapp-um<version>.x86_64.rpm
```

6. Execute o script de pré-instalação para garantir que não haja configurações de sistema ou qualquer software instalado que possa entrar em conflito com a instalação do Unified Manager:

```
sudo ./pre_install_check.sh
```

O script de pré-instalação verifica se o sistema tem uma assinatura válida do Red Hat Enterprise Linux e se ele tem acesso aos repositórios de software necessários. Se o script identificar quaisquer problemas, você deve corrigir os problemas antes de instalar o Unified Manager.

Para o sistema Red Hat Enterprise Linux 8, se você tiver repositórios internos com JDK 11 - OpenJDK, p7zip e outros pacotes de software fornecidos pelo repositório AppStream, você deve desativar o repositório AppStream e instalar o MySQL Community Server. Execute o seguinte comando:

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install  
mysql-community-server
```

7. **Opcional:** você deve executar o passo 7 somente se o seu sistema não estiver conectado à internet e você tiver que baixar manualmente os pacotes necessários para a sua instalação. Se o seu sistema tiver acesso à Internet e todos os pacotes necessários estiverem disponíveis, vá para o passo 8. Para sistemas que não estejam conectados à Internet ou que não estejam usando os repositórios Red Hat Enterprise Linux, execute as etapas a seguir para determinar se você está faltando algum pacote necessário e, em seguida, faça o download desses pacotes:

- a. No sistema em que você está instalando o Unified Manager, veja a lista de pacotes disponíveis e indisponíveis

```
yum install netapp-um<version>.x86_64.rpm --assumeno
```

Os itens na seção "Instalando:" são os pacotes que estão disponíveis no diretório atual, e os itens na seção "Instalando para dependências:" são os pacotes que estão faltando no seu sistema.

- b. Em um sistema que tenha acesso à Internet, baixe os pacotes ausentes:

```
yum install <package_name> --downloadonly --downloadaddir=.
```



Como o plug-in "yum-plugin-downloadonly" nem sempre está ativado em sistemas Red Hat Enterprise Linux, você pode precisar habilitar a funcionalidade para baixar um pacote sem instalá-lo:

```
yum install yum-plugin-downloadonly
```

a. Copie os pacotes ausentes do sistema conectado à Internet para o sistema de instalação.

8. Como usuário raiz, ou usando `sudo`, execute o seguinte comando para instalar o software:

```
yum install netapp-um<version>.x86_64.rpm
```

Este comando instala os pacotes `.rpm`, todos os outros softwares de suporte necessários e o software Unified Manager.

Se a instalação falhar com o erro GPG NOKEY, use `rpm --import` para importar as chaves de um URL:

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022
```



Não tente instalar usando comandos alternativos (como `rpm -ivh`). Uma instalação bem-sucedida do Unified Manager em um sistema Red Hat Enterprise Linux requer que todos os arquivos do Unified Manager e arquivos relacionados sejam instalados em uma ordem específica em uma estrutura de diretório específica que é aplicada automaticamente pelo `yum install netapp-um<version>.x86_64.rpm` comando.

9. Ignore a notificação de e-mail exibida imediatamente após as mensagens de instalação.

O e-mail notifica o usuário raiz de uma falha inicial do cron job, o que não tem efeito adverso na instalação.

10. Depois que as mensagens de instalação estiverem concluídas, role para trás pelas mensagens até que você veja a mensagem na qual o sistema exibe um endereço IP ou URL para a IU da Web do Unified Manager, o nome do usuário de manutenção (`umadmin`) e uma senha padrão.

A mensagem é semelhante à seguinte:

```
Active IQ Unified Manager installed successfully.
Use a web browser and one of the following URL(s) to configure and
access the Unified Manager GUI.
https://default_ip_address/      (if using IPv4)
https://[default_ip_address]/    (if using IPv6)
https://fully_qualified_domain_name/

Log in to Unified Manager in a web browser by using following details:
  username: umadmin
  password: admin
```

11. Registre o endereço IP ou URL, o nome de usuário atribuído (`umadmin`) e a senha atual.



12. Se você criou uma conta de usuário `umadmin` com um diretório inicial personalizado antes de instalar o Unified Manager, você deve especificar o shell de login do usuário `umadmin`:

```
usermod -s /bin/maintenance-user-shell.sh umadmin
```

Acesse a IU da Web para alterar a senha padrão do usuário `umadmin` e execute a configuração inicial do Unified Manager, conforme descrito em "[Configurando o Active IQ Unified Manager](#)". É obrigatório alterar a senha padrão do usuário `umadmin`.

### Usuários criados durante a instalação do Unified Manager

Quando você instala o Unified Manager no Red Hat Enterprise Linux, os seguintes usuários são criados pelo Unified Manager e utilitários de terceiros: `umadmin`, `jboss` e `mysql`.

- **umadmin**

Usado para fazer login no Unified Manager pela primeira vez. A este usuário é atribuída uma função de usuário "Administrador de aplicativos" e é configurada como o tipo "Usuário de Manutenção". Esse usuário é criado pelo Unified Manager.

- **jboss**

Usado para executar serviços do Unified Manager relacionados ao utilitário JBoss. Esse usuário é criado pelo Unified Manager.

- **mysql**

Usado para executar consultas de banco de dados MySQL do Unified Manager. Este usuário é criado pelo utilitário de terceiros MySQL.

Além desses usuários, o Unified Manager também cria grupos correspondentes: `Maintenance`, `jboss` e `mysql`. Os grupos de manutenção e `jboss` são criados pelo Unified Manager, enquanto o grupo `mysql` é criado por um utilitário de terceiros.



Se você criou um diretório inicial personalizado e definiu sua própria senha de usuário `umadmin` antes de instalar o Unified Manager, o programa de instalação não recriará o grupo de manutenção ou o usuário `umadmin`.

### Alterar a senha do JBoss

Você pode redefinir a senha JBoss específica da instância definida durante a instalação. Você pode redefinir a senha opcionalmente, caso seu site exija esse recurso de segurança para substituir a configuração de instalação do Unified Manager. Esta operação também altera a senha que o JBoss usa para acessar o MySQL.

- Você deve ter acesso de usuário raiz ao sistema Red Hat Enterprise Linux no qual o Unified Manager está instalado.
- Você deve ser capaz de acessar o script fornecido pelo NetApp `password.sh` no diretório `/opt/netapp/essentials/bin`.

## Passos

1. Inicie sessão como utilizador raiz no sistema.
2. Pare os serviços do Unified Manager inserindo os seguintes comandos na ordem mostrada:

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

Não pare o software MySQL associado.

3. Digite o seguinte comando para iniciar o processo de alteração de senha:

```
/opt/netapp/essentials/bin/password.sh resetJBossPassword
```

4. Quando solicitado, digite a nova senha do JBoss e insira-a uma segunda vez para confirmação.

Observe que a senha deve ter entre 8 e 16 caracteres, e deve conter pelo menos um dígito, caracteres maiúsculos e minúsculos e pelo menos um desses caracteres especiais:

```
!@%^*-_=[]:<>./~/+
```

5. Quando o script for concluído, inicie os serviços do Unified Manager inserindo os seguintes comandos na ordem mostrada:

```
systemctl start ocie
```

```
systemctl start ocieau
```

6. Depois que todos os serviços forem iniciados, você poderá fazer login na IU do Unified Manager.

## Atualização do Unified Manager no Red Hat Enterprise Linux

Você pode atualizar o Unified Manager quando uma nova versão estiver disponível.

As versões de patch do software Unified Manager, quando fornecidas pelo NetApp, são instaladas usando o mesmo procedimento que as novas versões.

Se o Unified Manager estiver emparelhado com uma instância do OnCommand Workflow Automation e houver novas versões de software disponíveis para ambos os produtos, será necessário desconectar os dois produtos e configurar uma nova conexão do Workflow Automation após a realização das atualizações. Se você estiver executando uma atualização para apenas um dos produtos, deverá fazer login no Workflow Automation após a atualização e verificar se ele ainda está adquirindo dados do Unified Manager.

### Caminho de atualização suportado para versões do Unified Manager

O Active IQ Unified Manager suporta um caminho de atualização específico para cada versão.

Nem todas as versões do Unified Manager podem realizar uma atualização no local para versões posteriores. As atualizações do Unified Manager estão limitadas a um modelo N-2, o que significa que uma atualização só pode ser realizada nas próximas versões do 2 em todas as plataformas. Por exemplo, você pode fazer uma atualização para o Unified Manager 9,16 somente do Unified Manager 9,13 e 9,14.

Se você estiver executando uma versão anterior às versões suportadas, sua instância do Unified Manager precisará ser atualizada primeiro para uma das versões suportadas e, em seguida, atualizada para a versão atual.

Por exemplo, se a versão instalada for o Unified Manager 9,9 e você quiser atualizar para o Unified Manager 9,14, siga uma sequência de atualizações.

#### **Exemplo de caminho de atualização:**

1. Atualização 9,11 → 9,13
2. Atualização 9,13 → 9,14
3. Atualização 9,14 → 9,16

Para obter mais informações sobre a matriz de caminho de atualização, consulte este ["artigo da base de conhecimento \(KB\)"](#).

### **Atualizando o Unified Manager**

Você pode atualizar do Unified Manager 9,13 ou 9,14 para 9,16 baixando e executando o arquivo de instalação na plataforma Linux.

#### **Antes de começar**

- O sistema no qual você está atualizando o Unified Manager deve atender aos requisitos de sistema e software.

["Requisitos do sistema de hardware"](#)Consulte .

["Requisitos de software e instalação do Linux"](#)Consulte .

- Você precisa ter uma assinatura do Red Hat Enterprise Linux Subscription Manager.
- Você deve instalar ou atualizar para a versão correta do OpenJDK antes de atualizar o Unified Manager.

["Atualizando o JRE no Linux"](#)Consulte .

- Para evitar a perda de dados, você deve ter criado um backup do banco de dados do Unified Manager caso haja algum problema durante a atualização. O NetApp recomenda que você mova o arquivo de backup do `/opt/netapp/data` diretório para um local externo.
- Durante a atualização, você pode ser solicitado a confirmar se deseja manter as configurações padrão anteriores para reter dados de desempenho por 13 meses ou alterá-los para 6 meses. Ao confirmar, os dados históricos de desempenho são purgados após 6 meses.
- Você deve ter concluído todas as operações em execução, pois o Unified Manager não está disponível durante o processo de atualização.
- O MySQL Community Edition é atualizado automaticamente durante a atualização do Unified Manager. Se a versão instalada do MySQL no seu sistema for anterior à 8,0.37, o processo de atualização do Unified Manager atualizará automaticamente o MySQL para 8,0.37.

#### **Passos**

1. Faça login no servidor Red Hat Enterprise Linux de destino.
2. Faça o download do pacote Unified Manager para o servidor.

["Baixando Unified Manager para Linux"](#)Consulte .

3. Navegue até o diretório de destino e expanda o pacote do Unified Manager:

```
unzip ActiveIQUnifiedManager-<version>.zip
```

Os módulos RPM necessários para o Unified Manager são descompactados no diretório de destino.

4. Verifique se o seguinte módulo está disponível no diretório:

```
ls *.rpm  
  
netapp-um<version>.x86_64.rpm
```

5. Execute o script de pré-instalação para garantir que não há configurações de sistema ou qualquer software instalado que possa entrar em conflito com a atualização:

```
sudo ./pre_install_check.sh
```

O script de pré-instalação verifica se o sistema tem uma assinatura válida do Red Hat Enterprise Linux e se ele tem acesso aos repositórios de software necessários. Se o script identificar quaisquer problemas, você deve corrigir os problemas e continuar com a atualização.

Se houver algum pacote ausente detectado, execute as etapas mencionadas em "[Etapas adicionais a serem executadas para pacotes ausentes](#)". Se não houver pacotes ausentes, continue com as próximas etapas.

6. Atualize o Unified Manager usando o seguinte script:

```
upgrade.sh
```

Esse script executa automaticamente os módulos RPM, atualizando o software de suporte necessário e os módulos do Unified Manager que são executados neles. Além disso, o script de atualização verifica se há configurações de sistema ou qualquer software instalado que possa entrar em conflito com a atualização. Se o script identificar quaisquer problemas, você deve corrigir os problemas antes de atualizar o Unified Manager. Se você tiver pacotes instalados anteriormente, como *net-snmp* antes de atualizar o Unified Manager, a dependência do MySQL pode desinstalar o pacote durante a atualização. Você precisa instalar o pacote manualmente novamente para continuar a usá-lo.

7. Depois que a atualização estiver concluída, role para trás pelas mensagens até que a mensagem exiba um endereço IP ou URL para a IU da Web do Unified Manager, o nome do usuário de manutenção (umadmin) e a senha padrão.

A mensagem é semelhante à seguinte:

```
Active IQ Unified Manager upgraded successfully.  
Use a web browser and one of the following URLs to access the Unified  
Manager GUI:  
  
https://default_ip_address/      (if using IPv4)  
https://[default_ip_address]/    (if using IPv6)  
https://fully_qualified_domain_name/
```

Insira o endereço IP ou URL especificado em uma nova janela de um navegador da Web compatível para iniciar a IU da Web do Unified Manager e, em seguida, faça login usando o mesmo nome de usuário de manutenção (umadmin) e senha definidos anteriormente.

### Etapas adicionais a serem executadas para pacotes ausentes

Se houver algum pacote ausente detectado em seu site durante a atualização, ou se seu sistema não estiver conectado à Internet, ou se você não estiver usando os repositórios Red Hat Enterprise Linux, execute as etapas a seguir para determinar se você está faltando quaisquer pacotes necessários e baixe esses pacotes.



Estas etapas precisam ser executadas após a etapa 5 do procedimento principal. Este procedimento atualiza o Unified Manager e você não precisa executar nenhuma etapa adicional para atualização.

1. Veja a lista de pacotes disponíveis e indisponíveis:

```
yum install netapp-um<version>.x86_64.rpm --assumeno
```

Os itens na seção "Instalando:" são os pacotes que estão disponíveis no diretório atual, e os itens na seção "Instalando para dependências:" são os pacotes que estão faltando no seu sistema.

2. Em um sistema diferente que tem o acesso à Internet, execute o seguinte comando para baixar os pacotes ausentes.

```
yum install package_name --downloadonly --downloaddir=.
```

Os pacotes são baixados no diretório especificado como --downloaddir=.

Como o plug-in "yum-plugin-downloadonly" nem sempre está ativado em sistemas Red Hat Enterprise Linux, você pode precisar habilitar a funcionalidade para baixar um pacote sem instalá-lo:

```
yum install yum-plugin-downloadonly
```

3. Copie os pacotes baixados para o diretório em que você descompactou o pacote Unified Manager no sistema de instalação.
4. Mude os diretórios para esse diretório e execute o seguinte comando para instalar os pacotes ausentes, juntamente com suas dependências.

```
yum install *.rpm
```

5. Inicie o servidor do Unified Manager. Execute estes comandos:

```
systemctl start ocie
```

```
systemctl start ocieau
```

Esse processo conclui o processo de atualização do Unified Manager. Insira o endereço IP ou URL especificado em uma nova janela de um navegador da Web compatível para iniciar a IU da Web do Unified Manager e, em seguida, faça login usando o mesmo nome de usuário de manutenção (umadmin) e senha definidos anteriormente.

## Atualizando o sistema operacional do host do Red Hat Enterprise Linux 7.x para 8.x

Se você já instalou o Unified Manager em um sistema Red Hat Enterprise Linux 7.x e precisa atualizar para o Red Hat Enterprise Linux 8.x, siga um dos procedimentos listados neste tópico. Em ambos os casos, você deve criar um backup do Unified Manager no sistema Red Hat Enterprise Linux 7.x e, em seguida, restaurar o backup em um sistema Red Hat Enterprise Linux 8.x. Observe que as versões suportadas do Red Hat Enterprise Linux são de 8,0 a 8,10.

A diferença entre as duas opções listadas abaixo é que, em um caso, você está executando a restauração do Unified Manager em um novo servidor 8.x e, no outro caso, você está executando a operação de restauração no mesmo servidor.

Como essa tarefa exige que você crie um backup do Unified Manager no sistema Red Hat Enterprise Linux 7.x, você deve criar o backup somente quando estiver preparado para concluir todo o processo de atualização para que o Unified Manager fique offline pelo menor período de tempo. As lacunas nos dados coletados aparecem na IU do Unified Manager pelo período de tempo durante o qual o sistema Red Hat Enterprise Linux 7.x é desligado e antes do novo Red Hat Enterprise Linux 8.x ser iniciado.

Veja "[Gerenciamento de operações de backup e restauração](#)" se você precisa revisar instruções detalhadas para os processos de backup e restauração.

Siga estas etapas se você tiver um sistema sobressalente no qual possa instalar o software Red Hat Enterprise Linux 8.x para que possa executar a restauração do Unified Manager nesse sistema enquanto o sistema Red Hat Enterprise Linux 7.x ainda estiver disponível.

1. Instale e configure um novo servidor com o software Red Hat Enterprise Linux 8.x.

"[Requisitos de software e instalação do Linux](#)"Consulte .

2. No sistema Red Hat Enterprise Linux 8.x, instale a mesma versão do software Unified Manager que você tem no sistema Red Hat Enterprise Linux 7.x.

"[Instalar o Unified Manager no Linux](#)"Consulte .

Não inicie a IU nem configure clusters, usuários ou configurações de autenticação quando a instalação estiver concluída. O arquivo de backup preenche essas informações durante o processo de restauração.

3. No sistema Red Hat Enterprise Linux 7.x, no menu Administration (Administração) na IU da Web, crie um backup do Unified Manager e, em seguida, copie o arquivo de backup(. 7z) e o conteúdo do subdiretório do repositório do banco de dados(/database-dumps-repo) para um local externo.
4. No sistema Red Hat Enterprise Linux 7.x, encerre o Unified Manager.
5. No sistema Red Hat Enterprise Linux 8.x, copie o arquivo de backup(. 7z) do local externo para /opt/netapp/data/ocum-backup/ os arquivos do repositório do banco de dados para /database-dumps-repo o subdiretório sob o /ocum-backup diretório.
6. Digite o seguinte comando para restaurar o banco de dados do Unified Manager a partir do arquivo de backup:

```
um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
```

7. Insira o endereço IP ou URL no navegador da Web para iniciar a IU da Web do Unified Manager e, em seguida, faça login no sistema.

Depois de verificar se o sistema está funcionando corretamente, você pode remover o Unified Manager do sistema Red Hat Enterprise Linux 7.x.

### Atualizando o sistema operacional do host no mesmo servidor

Siga estas etapas se você não tiver um sistema sobressalente no qual você pode instalar o software Red Hat Enterprise Linux 8.x.

1. No menu Administration (Administração) na IU da Web, crie um backup do Unified Manager e copie o arquivo de backup(.7z) e o conteúdo do subdiretório do diretório do repositório do banco de dados(/database-dumps-repo) para um local externo.
2. Remova a imagem Red Hat Enterprise Linux 7.x do sistema e limpe completamente o sistema.
3. Instale e configure o software Red Hat Enterprise Linux 8.x no mesmo sistema.

["Requisitos de software e instalação do Linux"](#)Consulte .

4. No sistema Red Hat Enterprise Linux 8.x, instale a mesma versão do software Unified Manager que você tinha no sistema Red Hat Enterprise Linux 7.x.

["Instalar o Unified Manager no Linux"](#)Consulte .

Não inicie a IU nem configure clusters, usuários ou configurações de autenticação quando a instalação estiver concluída. O arquivo de backup preenche essas informações durante o processo de restauração.

5. Copie o arquivo de (.7z`backup) do local externo para ``/opt/netapp/data/ocum-backup/`` e os arquivos do repositório do banco de dados para o `/database-dumps-repo` subdiretório sob o `/ocum-backup` diretório.
6. Digite o seguinte comando para restaurar o banco de dados do Unified Manager a partir do arquivo de backup:

```
um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
```

7. Insira o endereço IP ou URL no navegador da Web para iniciar a IU da Web do Unified Manager e, em seguida, faça login no sistema.

### Atualização de produtos de terceiros após a instalação do Unified Manager

Você pode atualizar produtos de terceiros, como JRE, quando o Unified Manager já estiver instalado em sistemas Linux.

As empresas que desenvolvem esses produtos de terceiros relatam vulnerabilidades de segurança regularmente. Você pode atualizar para versões mais recentes deste software em sua própria programação.

#### Atualizando o OpenJDK no Linux

Você pode atualizar para uma versão mais recente do OpenJDK no servidor Linux no qual o Unified Manager está instalado para obter correções para vulnerabilidades de segurança.

#### Antes de começar

Você precisa ter o Privileges raiz para o sistema Linux no qual o Unified Manager está instalado.

Você pode atualizar as versões do OpenJDK dentro das famílias de lançamento. Por exemplo, você pode atualizar do OpenJDK 11.0.14 para o OpenJDK 11,0.17, mas não pode atualizar diretamente do OpenJDK 11 para o OpenJDK 12.

### Passos

1. Faça login como usuário raiz na máquina host do Unified Manager.
2. Baixe a versão apropriada do OpenJDK (64 bits) para o sistema de destino.
3. Pare os serviços do Unified Manager:

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

4. Instale o OpenJDK mais recente no sistema.
5. Inicie os serviços do Unified Manager:

```
systemctl start ocie
```

```
systemctl start ocieau
```

## Reiniciando o Unified Manager

Talvez seja necessário reiniciar o Unified Manager depois de fazer alterações de configuração.

### Antes de começar

Você deve ter acesso de usuário raiz ao servidor Red Hat Enterprise Linux no qual o Unified Manager está instalado.

### Passos

1. Faça login como usuário raiz no servidor no qual você deseja reiniciar o serviço Unified Manager.
2. Pare o serviço Unified Manager e o serviço MySQL associado nesta ordem:

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

```
systemctl stop mysqld
```

3. Inicie os serviços MySQL e Unified Manager nesta ordem:

```
systemctl start mysqld
```

```
systemctl start ocie
```

```
systemctl start ocieau
```



mysqld É um programa daemon necessário para iniciar e parar o servidor MySQL.



## Remoção do Unified Manager

Você pode parar e desinstalar o Unified Manager do host Red Hat Enterprise Linux com um único comando.

### Antes de começar

- Você deve ter acesso de usuário raiz ao servidor a partir do qual deseja remover o Unified Manager.
- O Security-Enhanced Linux (SELinux) deve ser desativado no sistema Linux. Altere o modo de tempo de execução do SELinux para "permissivo" usando o `setenforce 0` comando.
- Todos os clusters (fontes de dados) devem ser removidos do servidor do Unified Manager antes de remover o software.
- Você deve excluir manualmente as regras de firewall criadas para permitir ou bloquear a porta MySQL 3306. As regras de firewall não são excluídas automaticamente.

### Passos

1. Faça login como usuário raiz no servidor no qual você deseja remover o Unified Manager.
2. Pare e remova o Unified Manager do servidor:

```
rpm -e netapp-um
```

Esta etapa remove todos os pacotes RPM do NetApp associados. Ele não remove os módulos de software pré-requisito, como Java, MySQL e p7zip.

3. **Opcional:** se apropriado, remova os módulos de software de suporte, como Java, MySQL e p7zip:

```
rpm -e p7zip mysql-community-client mysql-community-server mysql-community-common mysql-community-libs java-x.y
```

Após a conclusão desta operação, o software é removido. Todos os dados do `/opt/netapp/data` diretório são movidos para `/opt/netapp/data/BACKUP` a pasta após a desinstalação. A desinstalação do Unified Manager também remove os pacotes Java e MySQL, a menos que os pacotes sejam necessários e usados por qualquer outra aplicação no sistema. No entanto, os dados MySQL não são excluídos.

## Removendo o usuário personalizado umadmin e o grupo de manutenção

Se você criou um diretório inicial personalizado para definir seu próprio usuário umadmin e conta de manutenção antes de instalar o Unified Manager, remova esses itens depois de desinstalar o Unified Manager.

A desinstalação padrão do Unified Manager não remove uma conta de usuário e manutenção personalizada do umadmin. Você deve excluir esses itens manualmente.

### Passos

1. Faça login como usuário raiz no servidor Red Hat Enterprise Linux.
2. Excluir o usuário umadmin:

```
userdel umadmin
```

3. Eliminar o grupo de manutenção:

groupdel maintenance

# Instale o Unified Manager em sistemas Windows

## Introdução ao Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente chamado Gerenciador Unificado de OnCommand) permite que você monitore e gerencie a integridade e a performance dos sistemas de storage da ONTAP com uma única interface. Você pode implantar o Unified Manager em um servidor Linux, em um servidor Windows ou como um dispositivo virtual em um host VMware.

Após concluir a instalação e adicionar os clusters que você deseja gerenciar, o Unified Manager fornece uma interface gráfica que exibe a capacidade, disponibilidade, proteção e status de performance dos sistemas de storage monitorados.

### Informações relacionadas

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

### O que o servidor Unified Manager faz

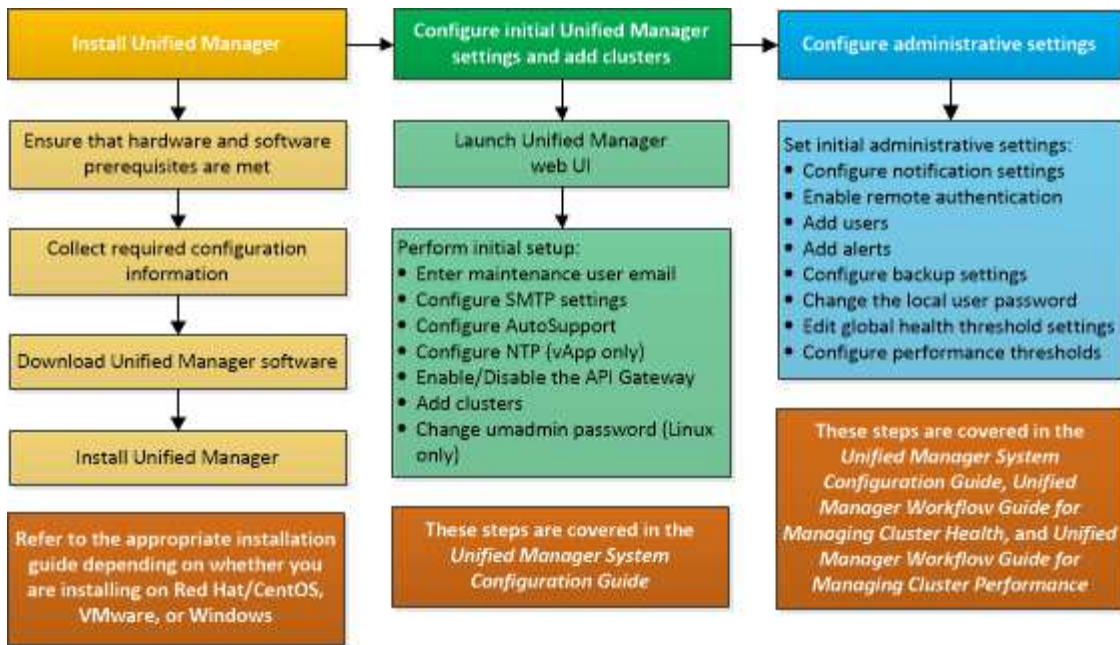
A infraestrutura de servidor do Unified Manager consiste em uma unidade de coleta de dados, um banco de dados e um servidor de aplicativos. Ele fornece serviços de infraestrutura como descoberta, monitoramento, controle de acesso baseado em funções (RBAC), auditoria e logs.

O Unified Manager coleta informações de cluster, armazena os dados no banco de dados e analisa os dados para verificar se há problemas de cluster.

### Descrição geral da sequência de instalação

O fluxo de trabalho de instalação descreve as tarefas que você deve executar antes de usar o Unified Manager.

Estas seções descrevem cada um dos itens mostrados no fluxo de trabalho abaixo.



## Requisitos para instalar o Unified Manager

Antes de iniciar o processo de instalação, verifique se o servidor no qual você deseja instalar o Unified Manager atende aos requisitos específicos de software, hardware, CPU e memória.

O NetApp não oferece suporte a nenhuma modificação do código do aplicativo do Unified Manager. Se você precisar aplicar quaisquer medidas de segurança ao servidor do Unified Manager, faça essas alterações no sistema operacional no qual o Unified Manager está instalado.

Para obter mais detalhes sobre como aplicar medidas de segurança ao servidor do Unified Manager, consulte o artigo da base de dados de Conhecimento.

["Capacidade de suporte para medidas de segurança aplicadas ao Active IQ Unified Manager for Clustered Data ONTAP"](#)

### Informações relacionadas

["Ferramenta de Matriz de interoperabilidade do NetApp"](#)

## Requisitos de infraestrutura virtual e sistema de hardware

A instalação do Unified Manager em uma infraestrutura virtual ou em um sistema físico deve atender aos requisitos mínimos de memória, CPU e espaço em disco.

A tabela a seguir exibe os valores recomendados para recursos de memória, CPU e espaço em disco. Esses valores foram qualificados para que o Unified Manager atenda aos níveis de desempenho aceitáveis.

Configuração de hardware	Definições recomendadas
RAM	12 GB (requisito mínimo de 8 GB)

Configuração de hardware	Definições recomendadas
Processadores	4 CPUs
Capacidade do ciclo da CPU	Total de 9572 MHz (requisito mínimo de 9572 MHz)
Espaço livre em disco	150 GB, onde a capacidade é alocada da seguinte forma: <ul style="list-style-type: none"> <li>• 100 GB de espaço em disco para o diretório de instalação</li> <li>• 50 GB de espaço em disco para o diretório de dados MySQL</li> </ul>

O Unified Manager pode ser instalado em sistemas com uma pequena quantidade de memória, mas os 12 GB de RAM recomendados garantem que haja memória suficiente disponível para um desempenho ideal e que o sistema possa acomodar clusters e objetos de armazenamento adicionais à medida que sua configuração cresce. Você não deve definir limites de memória na VM em que o Unified Manager é implantado e não deve habilitar recursos (por exemplo, balanceamento) que impeçam o software de utilizar a memória alocada no sistema.

Além disso, há um limite para o número de nós que uma única instância do Unified Manager pode monitorar antes de instalar uma segunda instância do Unified Manager. Para obter mais informações, consulte o *Guia de práticas recomendadas*.

["Relatório técnico 4621: Guia de práticas recomendadas do Unified Manager"](#)

A troca de páginas de memória afeta negativamente o desempenho do sistema e do aplicativo de gerenciamento. A concorrência por recursos de CPU indisponíveis devido à utilização geral do host pode degradar o desempenho.

### Requisito para uso dedicado

O sistema físico ou virtual no qual você instala o Unified Manager deve ser usado exclusivamente para o Unified Manager e não deve ser compartilhado com outros aplicativos. Outras aplicações podem consumir recursos do sistema e reduzir drasticamente a performance do Unified Manager.

### Requisitos de espaço para backups

Se você planeja usar o recurso de backup e restauração do Unified Manager, atribua capacidade adicional para que o diretório ou disco "data" tenha 150 GB de espaço. Um backup pode ser gravado em um destino local ou em um destino remoto. A prática recomendada é identificar um local remoto externo ao sistema host do Unified Manager que tenha no mínimo 150 GB de espaço.

### Requisitos para conectividade de host

O sistema físico ou o sistema virtual no qual você instala o Unified Manager deve ser configurado de tal forma que você possa obter com êxito `ping` o nome do host a partir do próprio host. No caso da configuração do IPv6, você deve verificar se `ping6` o nome do host é bem-sucedido para garantir que a instalação do Unified Manager seja bem-sucedida.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a IU da Web do produto. Se você

configurou um endereço IP estático para a rede durante a implantação, designou um nome para o host de rede. Se você configurou a rede usando DHCP, você deve obter o nome do host do DNS.

Se você pretende permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o nome de domínio totalmente qualificado (FQDN) ou o endereço IP, sua configuração de rede terá que resolver esse nome curto para um FQDN válido.

## Requisitos de software e instalação do Windows

Para a instalação bem-sucedida do Unified Manager no Windows, você deve garantir que o sistema no qual o Unified Manager está sendo instalado atenda aos requisitos de software.

### Software do sistema operativo

Você pode instalar o Unified Manager nas seguintes edições do Windows:

- Microsoft Windows Server 2019 Standard e Datacenter Edition
- Microsoft Windows Server 2022 Standard e Datacenter Edition

O Unified Manager é compatível com o sistema operacional Windows de 64 bits para os seguintes idiomas:

- Inglês
- Japonês
- Chinês simplificado

Consulte a Matriz de interoperabilidade para obter a lista completa e mais atual de versões suportadas do Windows.

["mysupport.NetApp.com/matrix"](https://mysupport.netapp.com/matrix)



O NetApp não oferece suporte à instalação do Gerenciador Unificado usando ferramentas de terceiros, como o Gerenciador de Configuração do Centro de sistema (SCCM) da Microsoft.

O servidor deve ser dedicado à execução do Unified Manager. Nenhum outro aplicativo deve ser instalado no servidor. É possível que um software antivírus ativo esteja instalado em seu sistema Windows por causa dos regulamentos da empresa. Você deve desativar o software antivírus antes de instalar o Unified Manager para evitar que a instalação falhe.

### Software de terceiros

Os seguintes pacotes de terceiros são empacotados com o Unified Manager. Se esses pacotes de terceiros não estiverem instalados no sistema, o Unified Manager os instalará como parte da instalação.

- Microsoft Visual C& n.o 43;& n.o 43; Redistributable Packages for Visual Studio 2015 versão 14.26.28720.3
- MySQL Community Edition versão 8.0.37
- Python 3.12.4
- OpenJDK versão 11.0.23
- p7zip versão 23,01 ou posterior



A partir do Unified Manager 9,5, o OpenJDK é fornecido no pacote de instalação do Unified Manager e instalado automaticamente. O Oracle Java não é suportado a partir do Unified Manager 9,5.

Se o MySQL estiver pré-instalado, você deve garantir que:

- Ele está usando a porta padrão.
- Os bancos de dados de amostra não estão instalados.
- O nome do serviço é "MYSQL8".

O Unified Manager é implantado em um servidor web WildFly. O WildFly 26.1.3 é empacotado e configurado com o Unified Manager.



Você deve encerrar uma instância em execução do Unified Manager antes de atualizar qualquer software de terceiros. Depois que a instalação de software de terceiros estiver concluída, você poderá reiniciar o Unified Manager.

## Requisitos de instalação

- O Microsoft .NET 4,5.2, ou superior, deve ser instalado.
- O `temp` diretório deve ser configurado com 2 GB de espaço em disco para extrair os arquivos de instalação. Para verificar se o diretório foi criado, execute o seguinte comando na interface de linha de comando: `echo %temp%`
- Você deve reservar 2 GB de espaço em disco na unidade do Windows para armazenar em cache os arquivos MSI do Unified Manager.
- O Microsoft Windows Server no qual você deseja instalar o Unified Manager deve ser configurado com um nome de domínio totalmente qualificado (FQDN), de modo que `ping` as respostas ao nome do host e FQDN sejam bem-sucedidas.
- Você deve desativar o serviço de publicação na Web mundial do Microsoft IIS e garantir que as portas 80 e 443 são gratuitas.
- Você deve certificar-se de que a configuração do Host de sessão de Área de trabalho Remota para "Compatibilidade RDS do Windows Installer" esteja desativada durante a instalação.
- A porta UDP 514 deve ser livre e não deve ser usada por nenhum outro serviço.
- Você deve desativar todo o software antivírus em seu sistema antes de instalar o Unified Manager. Após a conclusão da instalação, certifique-se de excluir manualmente os seguintes caminhos da verificação antivírus:
  - Diretório de dados do Unified Manager, por exemplo, `C:\ProgramData\NetApp\OnCommandAppData\`
  - Diretório de instalação do Unified Manager, por exemplo, `\C:\Program Files\NetApp\`
  - Diretório de dados MySQL, por exemplo, `C:\ProgramData\MySQL\MySQLServerData`

## Navegadores suportados

Para acessar a IU da Web do Unified Manager, use um navegador compatível.

A Matriz de interoperabilidade tem a lista de versões suportadas do navegador.

["mysupport.NetApp.com/matrix"](https://mysupport.NetApp.com/matrix)

Para todos os navegadores, a desativação dos bloqueadores pop-up garante que os recursos do software sejam exibidos corretamente.

Se você planeja configurar o Unified Manager para autenticação SAML, para que um provedor de identidade (IDP) possa autenticar usuários, você deve verificar a lista de navegadores suportados pelo IDP também.

## Requisitos de protocolo e porta

As portas e protocolos necessários permitem a comunicação entre o servidor do Unified Manager e os sistemas de storage gerenciado, servidores e outros componentes.

### Conexões ao servidor do Unified Manager

Em instalações típicas, você não precisa especificar números de porta ao se conectar à IU da Web do Unified Manager, porque as portas padrão são sempre usadas. Por exemplo, como o Unified Manager sempre tenta executar em sua porta padrão, você pode digitar `https://<host>` em vez de `https://<host>:443`.

O servidor do Unified Manager usa protocolos específicos para acessar as seguintes interfaces:

Interface	Protocolo	Porta	Descrição
IU da Web do Unified Manager	HTTP	80	Usado para acessar a IU da Web do Unified Manager; redireciona automaticamente para a porta segura 443.
IU da Web do Unified Manager e programas que usam APIs	HTTPS	443	Usado para acessar com segurança a IU da Web do Unified Manager ou para fazer chamadas de API; as chamadas de API só podem ser feitas usando HTTPS.
Consola de manutenção	SSH/SFTP	22	Usado para acessar o console de manutenção e recuperar pacotes de suporte.
Linha de comando Linux	SSH/SFTP	22	Usado para acessar a linha de comando Red Hat Enterprise Linux e recuperar pacotes de suporte.



<b>Interface</b>	<b>Protocolo</b>	<b>Porta</b>	<b>Descrição</b>
Syslog	UDP	514	Utilizado para acessar a mensagens EMS baseadas em subscrição a partir de sistemas ONTAP e para criar eventos com base nas mensagens.
DESCANSO	HTTPS	9443	Usado para acessar eventos EMS baseados em API REST em tempo real a partir de sistemas ONTAP autenticados.
Banco de dados MySQL	MySQL	3306	Usado para habilitar o acesso aos Serviços de API do OnCommand Workflow Automation e do OnCommand ao Unified Manager.
AMQP QPID broker	TCP/IP	56072	Usado para comunicação de mensagens internas.
AMQP QPID broker	WebSocket sobre TCP	56080	Usado para ouvir nessa porta as mensagens recebidas do ONTAP (agente de nuvem).
AMQP QPID broker	WebSocket sobre TCP	56443	Usado para ouvir nessa porta as mensagens recebidas do ONTAP (agente em nuvem). A comunicação por essa porta suporta criptografia fornecida pelo TLS ou SSL.
AMQP QPID broker	HTTP	9000	Usado para iniciar a interface de UI de gerenciamento AMQP nesta página.



A porta padrão para MySQL, 3306, é restrita apenas ao localhost durante a instalação do Unified Manager em sistemas Windows. Ative o firewall para restringir o acesso à porta MySQL, 3306, uma vez concluída a instalação. Isso não afeta nenhum cenário de atualização, onde a configuração anterior é mantida. Esta configuração pode ser modificada e a conexão pode ser disponibilizada a outros hosts usando a `Control access to MySQL port 3306` opção no console de manutenção. Para obter informações, "[Opções de menu adicionais](#)" consulte . As portas usadas para comunicação HTTP e HTTPS (portas 80 e 443) podem ser alteradas usando o console de manutenção do Unified Manager. Para obter mais informações, "[Configurando o Active IQ Unified Manager](#)" consulte .

## Conexões do servidor do Unified Manager

Você deve configurar seu firewall para abrir portas que habilitem a comunicação entre o servidor do Unified Manager e sistemas de armazenamento gerenciados, servidores e outros componentes. Se uma porta não estiver aberta, a comunicação falhará.

Dependendo do seu ambiente, você pode optar por modificar as portas e protocolos usados pelo servidor do Unified Manager para se conectar a destinos específicos.

O servidor Unified Manager se conecta, usando os seguintes protocolos e portas, aos sistemas de storage gerenciado, servidores e outros componentes:

Destino	Protocolo	Porta	Descrição
Sistema de storage	HTTPS	443/TCP	Usado para monitorar e gerenciar sistemas de storage.
Sistema de storage	NDMP	10000/TCP	Usado para certas operações de restauração do Snapshot.
Servidor AutoSupport	HTTPS	443	Usado para enviar informações do AutoSupport. Requer o acesso à Internet para executar esta função.
Servidor de autenticação	LDAP	389	Usado para fazer solicitações de autenticação e solicitações de pesquisa de usuários e grupos.
LDAPS	636	Usado para comunicação LDAP segura.	Servidor de correio
SMTP	25	Usado para enviar e-mails de notificação de alerta.	Emissor de trap SNMP

Destino	Protocolo	Porta	Descrição
SNMPv1 ou SNMPv3	162/UDP	Usado para enviar armadilhas SNMP de notificação de alerta.	Servidor de provedor de dados externo
TCP	2003	Usado para enviar dados de desempenho para um provedor de dados externo, como o Graphite.	Servidor NTP
NTP	123/UDP	Usado para sincronizar a hora no servidor do Unified Manager com um servidor de hora NTP externo. (Somente sistemas VMware)	AMQP QPID broker
TCP/IP	56072	Usado para comunicação de mensagens internas.	AMQP QPID broker
WebSocket sobre TCP	56080	Usado para ouvir nessa porta as mensagens recebidas do ONTAP (agente de nuvem).	AMQP QPID broker

## Completar a folha de trabalho

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

### Informações de instalação do Unified Manager

Os detalhes necessários para instalar o Unified Manager.

Sistema no qual o software é implantado	O seu valor
Host nome de domínio totalmente qualificado	
Endereço IP do host	
Máscara de rede	
Endereço IP do gateway	
Endereço DNS primário	

<b>Sistema no qual o software é implantado</b>	<b>O seu valor</b>
Endereço DNS secundário	
Pesquisar domínios	
Nome de utilizador de manutenção	
Palavra-passe do utilizador de manutenção	

### **Informações de configuração do Unified Manager**


Os detalhes para configurar o Unified Manager após a instalação. Alguns valores são opcionais, dependendo da configuração.

<b>Definição</b>	<b>O seu valor</b>
Endereço de e-mail do usuário de manutenção	
Nome do host do servidor SMTP ou endereço IP	
Nome de utilizador SMTP	
Palavra-passe SMTP	
Porta de SMTP	25 (valor padrão)
E-mail a partir do qual as notificações de alerta são enviadas	
Nome do host ou endereço IP do servidor de autenticação	
Nome de administrador do ativo Directory ou nome distinto de associação LDAP	
Palavra-passe do ativo Directory ou palavra-passe LDAP BIND	
Nome distinto da base do servidor de autenticação	
URL do provedor de identidade (IDP)	
Metadados do provedor de identidade (IDP)	

Definição	O seu valor
Endereços IP do host de destino de intercetação SNMP	
Porta de SNMP	

### Informações do cluster

Os detalhes dos sistemas de storage que você gerencia usando o Unified Manager.

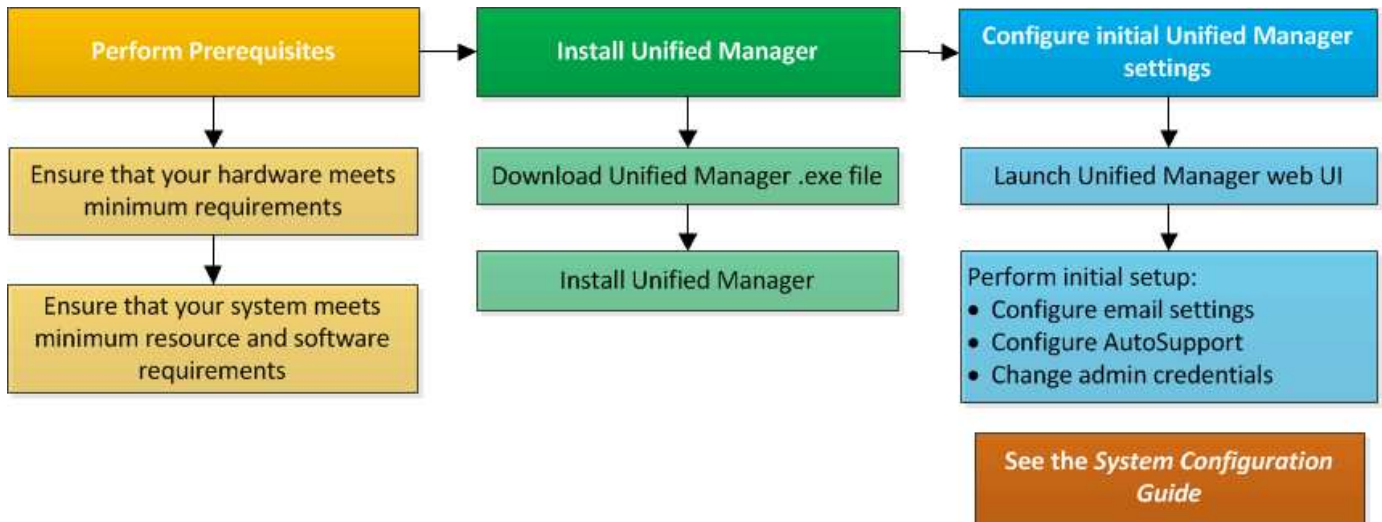
Cluster 1 de N	O seu valor
Nome do host ou endereço IP de gerenciamento de cluster	
Nome de usuário do administrador do ONTAP  O administrador deve ter sido atribuído a função "admin".	
Senha do administrador do ONTAP	
Protocolo	HTTPS

## Instalação, atualização e remoção do software Unified Manager

Você pode instalar o Unified Manager, atualizar para uma versão mais recente ou remover o aplicativo Unified Manager.

### Visão geral do processo de instalação

O fluxo de trabalho de instalação descreve as tarefas que você deve executar antes de usar o Unified Manager.



## Instalar o Unified Manager no Windows

É importante que você entenda a sequência de etapas para baixar e instalar o Unified Manager no Windows.

### Instalar o Unified Manager

É possível instalar o Unified Manager para monitorar e solucionar problemas de capacidade, disponibilidade, performance e proteção do storage de dados.

#### Antes de começar

- O sistema no qual você planeja instalar o Unified Manager deve atender aos requisitos de sistema e software.

"Requisitos do sistema de hardware"Consulte .

"Requisitos de software e instalação do Windows"Consulte .



A partir do Unified Manager 9,5, o OpenJDK é fornecido no pacote de instalação e instalado automaticamente. O Oracle Java não é suportado a partir do Unified Manager 9,5.

- Você deve ter o administrador do Windows Privileges. Certifique-se de que o seu nome de utilizador não começa com um ponto de exclamação "!". Installation of Unified Manager might fail if the user name of user running the installation begins with "!" !.
- Todos os clusters são compatíveis, com exceção dos sistemas ASA R2.
- Você deve ter um navegador da Web compatível.
- A senha do usuário de manutenção do Unified Manager deve ter entre 8 e 20 caracteres, deve conter letras maiúsculas ou minúsculas, números e caracteres especiais.
- Os seguintes caracteres especiais não são permitidos na cadeia de caracteres de senha para o usuário de manutenção ou para o usuário raiz MySQL: "

Os seguintes caracteres especiais são permitidos: \* - ? . Selecione a opção

#### Passos

1. Inicie sessão no Windows utilizando a conta de administrador local predefinida.
2. Faça login no site de suporte da NetApp e navegue até a página de download do Gerenciador Unificado:

["Site de suporte da NetApp"](#)

3. Selecione a versão necessária do Unified Manager e aceite o contrato de licença de usuários finais (EULA).
4. Transfira o ficheiro de instalação do Unified Manager Windows ou o ficheiro zip para um diretório de destino no sistema Windows.
5. Extraia o arquivo zip, se necessário, e navegue até o diretório onde o arquivo de instalação está localizado.
6. Clique com o botão direito do rato e execute o ficheiro executável (.exe) do instalador do Unified Manager como administrador.

O Unified Manager deteta pacotes de terceiros ausentes ou pré-instalados e os lista. Se os pacotes de terceiros necessários não estiverem instalados no sistema, o Unified Manager os instalará como parte da instalação.

7. Clique em **seguinte**.
8. Introduza o nome de utilizador e a palavra-passe para criar o utilizador de manutenção.
9. No assistente conexão de banco de dados, insira a senha raiz do MySQL.
10. Clique em **Change** para especificar um novo local para o diretório de instalação do Unified Manager e o diretório de dados MySQL.

Se você não alterar o diretório de instalação, o Unified Manager será instalado no diretório de instalação padrão.

11. Clique em **seguinte**.
12. No assistente Ready to Install Shield, clique em **Install**.
13. Após a conclusão da instalação, clique em **Finish**.
14. Se tiver um software antivírus ativo instalado no seu sistema Windows, exclua manualmente os seguintes caminhos da verificação antivírus após a conclusão da instalação:
  - Diretório de dados do Unified Manager
  - Diretório de instalação do Unified Manager
  - Diretório de dados MySQL

A instalação cria vários diretórios:

- Diretório de instalação

Este é o diretório raiz do Unified Manager, que você especificou durante a instalação. Exemplo:  
C:\Program Files\NetApp\

- Diretório de dados MySQL

Este é o diretório onde os bancos de dados MySQL são armazenados, que você especificou durante a instalação. Exemplo: C:\ProgramData\MySQL\MySQLServerData\

- Diretório Java

Este é o diretório onde o OpenJDK está instalado. Exemplo: C:\Program Files\NetApp\JDK\

- Diretório de dados do aplicativo do Unified Manager (appDataDir)

Este é o diretório onde todos os dados gerados pela aplicação são armazenados. Isso inclui logs, pacotes de suporte, backup e todos os outros dados adicionais. Exemplo:

C:\ProgramData\NetApp\OnCommandAppData\

Você pode acessar a IU da Web para executar a configuração inicial do Unified Manager, conforme descrito no ["Configurando o Active IQ Unified Manager"](#).

## Executando uma instalação autônoma do Unified Manager

Você pode instalar o Unified Manager sem a intervenção do usuário usando a interface de linha de comando. Você pode concluir a instalação autônoma passando os parâmetros em pares de valor-chave.

### Passos

1. Inicie sessão na interface da linha de comandos do Windows utilizando a conta de administrador local predefinida.
2. Navegue até o local onde deseja instalar o Unified Manager e escolha uma das seguintes opções:

Opção	Instruções
Se os pacotes de terceiros estiverem pré-instalados	<pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qn /l*v CompletePathForLogFile"</pre> <p><b>Exemplo:</b></p> <pre>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MySQL\MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qn /l*v C:\install.log"</pre>



Opção	Instruções
Se pacotes de terceiros não estiverem instalados	<pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR="Installation directory\" MYSQL_DATA_DIR="MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qr /l*v CompletePathForLogFile"  <b>Exemplo:</b>  ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR="C:\Program Files\NetApp\" MYSQL_DATA_DIR="C:\ProgramData\MySQL\ MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qr /l*v C:\install.log"</pre>

A /qr opção ativa o modo silencioso com uma interface de utilizador reduzida. É apresentada uma interface de utilizador básica, que mostra o progresso da instalação. Você não é solicitado a fornecer entradas. Se pacotes de terceiros, como JRE, MySQL e 7zip, não estiverem pré-instalados, você deve usar a /qr opção. A instalação falha se a /qn opção for usada em um servidor onde pacotes de terceiros não estão instalados.

A /qn opção ativa o modo silencioso sem interface de utilizador. Nenhuma interface do usuário ou detalhes são exibidos durante a instalação. Você não deve usar a /qn opção quando os pacotes de terceiros não estiverem instalados.

3. Faça login na interface de usuário da Web do Unified Manager usando o seguinte URL:

`https://IP address`

## Alterar a senha do JBoss

Você pode redefinir a senha JBoss específica da instância definida durante a instalação. Você pode redefinir a senha opcionalmente, caso seu site exija esse recurso de segurança para substituir a configuração de instalação do Unified Manager. Esta operação também altera a senha que o JBoss usa para acessar o MySQL.

### Antes de começar

- Você deve ter o Privileges de administrador do Windows para o sistema no qual o Unified Manager está instalado.
- Você deve ter a senha para o usuário root do MySQL.
- Você deve ser capaz de acessar o script fornecido pelo NetApp `password.bat` no diretório

`C:\Program Files\NetApp\essentials\bin.`

## Passos

1. Faça login como usuário admin na máquina host do Unified Manager.
2. Use o console dos Serviços do Windows para interromper os seguintes serviços do Unified Manager:
  - Serviço de aquisição da NetApp Active IQ (Ocie-au)
  - Serviço de servidor de gerenciamento NetApp Active IQ (Oncommandsvc)
3. Inicie o `password.bat` script para iniciar o processo de alteração de senha:

```
C:\Program Files\NetApp\essentials\bin> password.bat resetJBossPassword
```

4. Quando solicitado, insira a senha do usuário raiz do MySQL.
5. Quando solicitado, digite a nova senha de usuário do JBoss e insira-a novamente para confirmação.

Observe que a senha deve ter entre 8 e 16 caracteres, e deve conter pelo menos um dígito, caracteres maiúsculos e minúsculos e pelo menos um desses caracteres especiais:

```
!@%^*-_=[]:<>./~+
```

6. Quando o script for concluído, inicie os serviços do Unified Manager usando o console do Windows Services:
  - Serviço de servidor de gerenciamento NetApp Active IQ (Oncommandsvc)
  - Serviço de aquisição da NetApp Active IQ (Ocie-au)
7. Depois que todos os serviços forem iniciados, você poderá fazer login na IU do Unified Manager.

## Caminho de atualização suportado para versões do Unified Manager

O Active IQ Unified Manager suporta um caminho de atualização específico para cada versão.

Nem todas as versões do Unified Manager podem realizar uma atualização no local para versões posteriores. As atualizações do Unified Manager estão limitadas a um modelo N-2, o que significa que uma atualização só pode ser realizada nas próximas versões do 2 em todas as plataformas. Por exemplo, você pode fazer uma atualização para o Unified Manager 9,16 somente do Unified Manager 9,13 e 9,14.

Se você estiver executando uma versão anterior às versões suportadas, sua instância do Unified Manager precisará ser atualizada primeiro para uma das versões suportadas e, em seguida, atualizada para a versão atual.

Por exemplo, se a versão instalada for o Unified Manager 9,9 e você quiser atualizar para o Unified Manager 9,14, siga uma sequência de atualizações.

### Exemplo de caminho de atualização:

1. Atualização 9,11 → 9,13
2. Atualização 9,13 → 9,14
3. Atualização 9,14 → 9,16

Para obter mais informações sobre a matriz de caminho de atualização, consulte este ["artigo da base de conhecimento \(KB\)"](#).

## Atualizando o Unified Manager

Você pode atualizar o Unified Manager 9,13 ou 9,14 para 9,16 baixando e executando o arquivo de instalação na plataforma Windows.

### Antes de começar

- O sistema no qual você está atualizando o Unified Manager deve atender aos requisitos de sistema e software.

"Requisitos do sistema de hardware"Consulte .

"Requisitos de software e instalação do Windows"Consulte .



A partir do Unified Manager 9,5, o OpenJDK é fornecido no pacote de instalação e instalado automaticamente. O Oracle Java não é suportado a partir do Unified Manager 9,5.



Certifique-se de que o Microsoft .NET 4.5.2 ou superior esteja instalado no seu sistema antes de iniciar a atualização.

- O MySQL Community Edition é atualizado automaticamente durante a atualização do Unified Manager. Se a versão instalada do MySQL no seu sistema for anterior à 8,0.37, o processo de atualização do Unified Manager atualizará automaticamente o MySQL para 8,0.37. Você não deve executar uma atualização autônoma de uma versão anterior do MySQL para 8,0.37.
- Todos os clusters são compatíveis, com exceção dos sistemas ASA R2.
- Você deve ter o administrador do Windows Privileges. Certifique-se de que o seu nome de utilizador não começa com um ponto de exclamação "!". Installation of Unified Manager might fail if the user name of user running the installation begins with "" !".
- Você deve ter credenciais válidas para fazer login no site de suporte da NetApp.
- Para evitar a perda de dados, você deve ter criado um backup da máquina do Unified Manager caso haja algum problema durante a atualização.
- Você deve ter espaço em disco adequado disponível para realizar a atualização.

O espaço disponível na unidade de instalação deve ser 2,5 GB maior do que o tamanho do diretório de dados. A atualização pára e exibe uma mensagem de erro indicando a quantidade de espaço a ser adicionado se não houver espaço livre suficiente.

- Durante a atualização, você pode ser solicitado a confirmar se deseja manter as configurações padrão anteriores para reter dados de desempenho por 13 meses ou alterá-los para 6 meses. Ao confirmar, os dados históricos de desempenho após 6 meses são purgados.
- Antes de atualizar, você deve fechar todos os arquivos ou pastas abertos em *<InstallDir>* e *diretório de dados MySQL*.
- Se tiver um software antivírus ativo instalado no sistema Windows, a atualização do Unified Manager poderá falhar. Você deve desativar todo o software de verificação de vírus em seu sistema antes de atualizar o Unified Manager.

Durante o processo de atualização, o Unified Manager não está disponível. Você deve concluir todas as operações em execução antes de atualizar o Unified Manager.

Se o Unified Manager estiver emparelhado com uma instância do OnCommand Workflow Automation e houver novas versões de software disponíveis para ambos os produtos, será necessário desconectar os dois produtos

e configurar uma nova conexão do Workflow Automation após a realização das atualizações. Se você estiver executando uma atualização para apenas um dos produtos, deverá fazer login no Workflow Automation após a atualização e verificar se ele ainda está adquirindo dados do Unified Manager.

## Passos

1. Faça login no site de suporte da NetApp e navegue até a página de download do Gerenciador Unificado:

["Site de suporte da NetApp"](#).

2. Selecione a versão necessária do Unified Manager e aceite o contrato de licença de usuários finais (EULA).
3. Transfira o ficheiro de instalação do Unified Manager Windows ou o ficheiro zip para um diretório de destino no sistema Windows. Extraia o arquivo zip, se necessário, e navegue até o diretório onde o arquivo de instalação está localizado. Clique com o botão direito do rato e execute o ficheiro executável (.exe) do instalador do Unified Manager como administrador.

O Unified Manager solicita a seguinte mensagem:

```
This setup will perform an upgrade of Unified Manager. Do you want to continue?
```

4. Clique em **Yes** e, em seguida, clique em **Next**.
5. Digite a senha de root do MySQL8 que foi definida durante a instalação e clique em **Next**.
6. Inicie a IU da Web em uma nova janela em um navegador da Web compatível e faça login para usar a versão atualizada do Unified Manager.
7. Se tiver um software antivírus ativo instalado no sistema Windows, certifique-se de excluir manualmente os seguintes caminhos da verificação antivírus após a conclusão da atualização:
  - Diretório de dados do Unified Manager
  - Diretório de instalação do Unified Manager
  - Diretório de dados MySQL



Para executar uma atualização silenciosa do Unified Manager, execute o seguinte comando:  
`ActiveIQUnifiedManager-<version>.exe /s /v"MYSQL_PASSWORD=<password>  
/qn /l*v <system_drive>:\install.log"`

## Atualização de produtos de terceiros

Você pode atualizar produtos de terceiros, como JRE, no Unified Manager quando instalado em sistemas Windows.

As empresas que desenvolvem esses produtos de terceiros relatam vulnerabilidades de segurança regularmente. Você pode atualizar para versões mais recentes deste software em sua própria programação.

### Atualizando o OpenJDK

Você pode atualizar para uma versão mais recente do OpenJDK no servidor Windows no qual o Unified Manager está instalado para obter correções para vulnerabilidades de

segurança.

### Antes de começar

Você deve ter o Privileges de administrador do Windows para o sistema no qual o Unified Manager está instalado.

Você pode atualizar as versões do OpenJDK dentro das famílias de lançamento. Por exemplo, você pode atualizar do OpenJDK 11.0.16 para o OpenJDK 11,0.18, mas não pode atualizar diretamente do OpenJDK 11 para o OpenJDK 12.

### Passos

1. Faça login como usuário admin na máquina host do Unified Manager.
2. Baixe a versão apropriada do OpenJDK (64 bits) do site OpenJDK para o sistema de destino.

Por exemplo, faça o `jdk-11.0.18_windows-x64_bin.zip` from <https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html> download do .



Uma conta Oracle é necessária para baixar o arquivo. Se você não tiver uma conta Oracle, vá para "[Início de sessão da conta Oracle](#)" a página para criar uma.

3. Use o console dos Serviços do Windows para interromper os seguintes serviços do Unified Manager:
  - Serviço de aquisição da NetApp Active IQ (Ocie-au)
  - Serviço de servidor de gerenciamento NetApp Active IQ (Oncommandsvc)
4. Expanda o zip ficheiro.
5. Copie os diretórios e arquivos do diretório resultante `jdk` (por exemplo, `jdk-11.0.18` para o local onde o Java está instalado. Exemplo: `C:\Program Files\NetApp\JDK\`
6. Inicie os serviços do Unified Manager usando o console dos Serviços do Windows:
  - Serviço de servidor de gerenciamento NetApp Active IQ (Oncommandsvc)
  - Serviço de aquisição da NetApp Active IQ (Ocie-au)

## Desinstalar produtos de terceiros

Depois de atualizar o Unified Manager, você pode desinstalar produtos de terceiros, como Python ou Microsoft Visual C 2013. Isso é opcional.

### Desinstalar o Python

#### Passos

1. A partir do **Painel de controlo** selecione **programas > programas e funcionalidades**.
2. Selecione Python na lista de programas.
3. Selecione **Desinstalar este programa**. Desinstale qualquer versão do Python, exceto 3,12. Certifique-se de manter Python versão 3,12.

### Desinstalar o Microsoft Visual C 2013

#### Passos

1. A partir do **Painel de controlo** selecione **programas > programas e funcionalidades**.

2. Selecione **Microsoft Visual C 2013** na lista de programas.
3. Selecione **Desinstalar este programa**.

## Reiniciando o Unified Manager

Talvez seja necessário reiniciar o Unified Manager depois de fazer alterações de configuração.

### Antes de começar

Você deve ter o Privileges administrador do Windows.

### Passos

1. Inicie sessão no Windows utilizando a conta de administrador local predefinida.
2. Pare os serviços do Unified Manager:

A partir do...	Pare os serviços na seguinte ordem...
Linha de comando	<ol style="list-style-type: none"> <li>a. <code>sc stop ocie-au</code></li> <li>b. <code>sc stop Oncommandsvc</code></li> </ol>
Microsoft Service Manager	<ol style="list-style-type: none"> <li>a. Serviço de aquisição da NetApp Active IQ (Ocie-au)</li> <li>b. Serviço de servidor de gerenciamento NetApp Active IQ (Oncommandsvc)</li> </ol>

3. Inicie os serviços do Unified Manager:

A partir do...	Inicie os serviços na seguinte ordem...
Linha de comando	<ol style="list-style-type: none"> <li>a. <code>sc start Oncommandsvc</code></li> <li>b. <code>sc start ocie-au</code></li> </ol>
Microsoft Service Manager	<ol style="list-style-type: none"> <li>a. Serviço de servidor de gerenciamento NetApp Active IQ (Oncommandsvc)</li> <li>b. Serviço de aquisição da NetApp Active IQ (Ocie-au)</li> </ol>

## Desinstalar o Unified Manager

Você pode desinstalar o Unified Manager usando o assistente programas e recursos ou executando uma desinstalação autônoma da interface da linha de comando.

### Antes de começar

- Você deve ter o Privileges administrador do Windows.
- Todos os clusters (fontes de dados) devem ser removidos do servidor do Unified Manager antes de desinstalar o software.

- Você deve excluir manualmente as regras de firewall criadas para permitir ou bloquear a porta MySQL 3306. As regras de firewall não são excluídas automaticamente.

## Passos

1. Desinstale o Unified Manager escolhendo uma das seguintes opções:

- Se você desinstalar o Unified Manager do assistente **programas e recursos**, execute estas etapas:
  - i. Navegue até **Painel de Controle > Programa e recursos**.
  - ii. Selecione Active IQ Unified Manager e clique em **Desinstalar**.
- Se você desinstalar o Unified Manager da linha de comando, execute estas etapas:
  - i. Faça login na linha de comando do Windows usando o administrador Privileges.
  - ii. Navegue até o diretório Active IQ Unified Manager e execute o seguinte comando:

```
msiexec /x {A78760DB-7EC0-4305-97DB-E4A89CDFF4E1} /qn /l*v  
%systemdrive%\UmUnInstall.log
```

Se o Controle de conta de Usuário (UAC) estiver ativado no servidor e você estiver conectado como um usuário de domínio, você deverá usar o método de desinstalação da linha de comando.

O Unified Manager é desinstalado do sistema.

2. Desinstale os seguintes pacotes e dados de terceiros que não são removidos durante a desinstalação do Unified Manager:
- Pacotes de terceiros: JRE, MySQL, Microsoft Visual C& n.o 43;& n.o 43; 2015 Redistributable, Python e 7zip
  - Dados da aplicação MySQL gerados pelo Unified Manager
  - Registos de aplicações e conteúdos do diretório de dados da aplicação

# Executar tarefas de configuração e administrativas

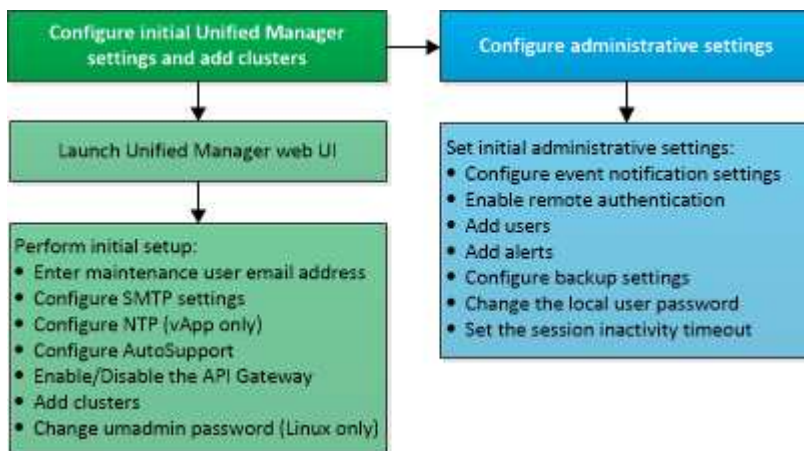
## Configurando o Active IQ Unified Manager

Depois de instalar o Active IQ Unified Manager (antigo Gerenciador Unificado do OnCommand), você deve concluir a configuração inicial (também chamada de assistente de primeira experiência) para acessar a IU da Web. Depois, você pode executar tarefas de configuração adicionais, como adicionar clusters, configurar autenticação remota, adicionar usuários e adicionar alertas.

Alguns dos procedimentos descritos neste manual são necessários para concluir a configuração inicial da instância do Unified Manager. Outros procedimentos são configurações recomendadas que são úteis para configurar em sua nova instância ou que são boas para saber antes de iniciar o monitoramento regular de seus sistemas ONTAP.

### Descrição geral da sequência de configuração

O fluxo de trabalho de configuração descreve as tarefas que você deve executar antes de usar o Unified Manager.



### Acessando a IU da Web do Unified Manager

Depois de instalar o Unified Manager, você pode acessar a IU da Web para configurar o Unified Manager para começar a monitorar seus sistemas ONTAP.

#### Antes de começar

- Se esta for a primeira vez que você estiver acessando a IU da Web, você deve fazer login como o usuário de manutenção (ou usuário umadmin para instalações Linux).
- Se você pretende permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o nome de domínio totalmente qualificado (FQDN) ou o endereço IP, sua configuração de rede deve resolver esse nome curto para um FQDN válido.
- Se o servidor usar um certificado digital autoassinado, o navegador poderá exibir um aviso indicando que o certificado não é confiável. Você pode reconhecer o risco de continuar o acesso ou instalar um certificado digital assinado pela autoridade de certificação (CA) para autenticação do servidor.



## Passos

1. Inicie a IU da Web do Unified Manager a partir do navegador usando o URL exibido no final da instalação. O URL é o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do servidor do Unified Manager.

O link está no seguinte formato: `https://URL`.

2. Faça login na IU da Web do Unified Manager usando suas credenciais de usuário de manutenção.



Se você fizer três tentativas consecutivas sem sucesso para fazer login na IU da Web dentro de uma hora, você será bloqueado para fora do sistema e precisará entrar em Contato com o administrador do sistema. Isto é aplicável apenas a utilizadores locais.

## Executando a configuração inicial da IU da Web do Unified Manager

Para usar o Unified Manager, você deve primeiro configurar as opções de configuração inicial, incluindo o servidor NTP, o endereço de e-mail do usuário de manutenção, o host do servidor SMTP e a adição de clusters ONTAP.

### Antes de começar

Você deve ter realizado as seguintes operações:

- Inicie a IU da Web do Unified Manager usando o URL fornecido após a instalação
- Logado usando o nome de usuário de manutenção e senha (usuário umadmin para instalações Linux) criados durante a instalação

A página Gerenciamento Unificado do Active IQ é exibida somente quando você acessa a IU da Web pela primeira vez. A página abaixo é de uma instalação na VMware.

## Getting Started



### Notifications

Configure your email server for assistance in case you forget your password.

### Maintenance User Email

Email

### SMTP Server

Host Name or IP Address

Port

User Name

Password

Use STARTTLS [i](#)  Use SSL [i](#)

**Continue**

Se você quiser alterar qualquer uma dessas opções posteriormente, selecione sua opção nas opções Gerais no painel de navegação esquerdo do Unified Manager. Observe que a configuração NTP é somente para instalações VMware e pode ser alterada posteriormente usando o console de manutenção do Unified Manager.

### Passos

1. Na página Configuração inicial do Active IQ Unified Manager, insira o endereço de e-mail do usuário de manutenção, o nome do host do servidor SMTP e quaisquer opções adicionais de SMTP e o servidor NTP (somente instalações VMware). Em seguida, clique em **continuar**.



Se você tiver selecionado a opção **Use STARTTLS** ou **Use SSL**, uma página de certificado será exibida após clicar no botão **Continue**. Verifique os detalhes do certificado e aceite o certificado para continuar com as configurações iniciais da IU da Web.

2. Na página AutoSupport, clique em **Concordo e continuar** para ativar o envio de mensagens do AutoSupport do Unified Manager para o NetAppactive IQ.

Se você precisar designar um proxy para fornecer acesso à Internet para enviar conteúdo AutoSupport ou se quiser desativar o AutoSupport, use a opção **Geral > AutoSupport** na interface da Web.

3. Nos sistemas Red Hat, altere a senha do usuário `umadmin` da cadeia padrão `"admin"` para uma cadeia personalizada.
4. Na página Configurar gateway de API, selecione se deseja usar o recurso de gateway de API que permite ao Gerenciador Unificado gerenciar os clusters do ONTAP que você está planejando monitorar usando APIs REST do ONTAP. Em seguida, clique em **continuar**.

Você pode ativar ou desativar essa configuração posteriormente na IU da Web em **Geral > Configurações de recursos > Gateway de API**. Para obter mais informações sobre as APIs, "[Primeiros passos com as APIs REST do Active IQ Unified Manager](#)" consulte .

5. Adicione os clusters que você deseja que o Unified Manager gerencie e clique em **Avançar**. Para cada cluster que você pretende gerenciar, você deve ter o nome do host ou o endereço IP de gerenciamento de cluster (IPv4 ou IPv6) juntamente com as credenciais de nome de usuário e senha - o usuário deve ter a função `"admin"`.

Este passo é opcional. Você pode adicionar clusters mais tarde na IU da Web em **Gerenciamento de armazenamento > Configuração de cluster**.

6. Na página Resumo, verifique se todas as configurações estão corretas e clique em **concluir**.

A página Introdução fecha-se e a página Painel do Unified Manager é exibida.

## Adição de clusters

Você pode adicionar um cluster ao Active IQ Unified Manager para que você possa monitorar o cluster. Isso inclui a capacidade de obter informações de cluster, como integridade, capacidade, desempenho e configuração do cluster, para que você possa encontrar e resolver quaisquer problemas que possam ocorrer.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter as seguintes informações:
  - O Unified Manager dá suporte a clusters ONTAP on-premises, ONTAP Select, Cloud Volumes ONTAP.
  - Nome do host ou endereço IP de gerenciamento de cluster

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

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

- O cluster deve estar executando o software ONTAP versão 9,1 ou superior.
- Nome de usuário e senha do administrador do ONTAP

Essa conta deve ter a função `admin` com acesso ao aplicativo definido como `ontapi`, `console` e `http`.

- O número da porta para se conectar ao cluster usando o protocolo HTTPS (normalmente a porta 443)
- Você tem os certificados necessários:

**Certificado SSL (HTTPS):** Este certificado pertence ao Unified Manager. Um certificado SSL (HTTPS)

autoassinado padrão é gerado com uma nova instalação do Unified Manager. A NetApp recomenda que você o atualize para um certificado assinado pela CA para obter uma melhor segurança. Se o certificado do servidor expirar, você deverá regenerá-lo e reiniciar o Unified Manager para que os serviços incorporem o novo certificado. Para obter mais informações sobre como regenerar o certificado SSL, "[Gerando um certificado de segurança HTTPS](#)" consulte .

**Certificado EMS:** Este certificado é de propriedade do Unified Manager. Ele é usado durante a autenticação para notificações EMS recebidas do ONTAP.

**Certificados para comunicação TLS mútua:** Usados durante a comunicação TLS mútua entre o Unified Manager e o ONTAP. A autenticação baseada em certificado é ativada para um cluster, com base na versão do ONTAP. Se o cluster que executa a versão do ONTAP for inferior à 9,5, a autenticação baseada em certificado não está ativada.

A autenticação baseada em certificado não será ativada automaticamente para um cluster, se você estiver atualizando uma versão mais antiga do Unified Manager. No entanto, você pode ativá-lo modificando e salvando os detalhes do cluster. Se o certificado expirar, você deve regenerá-lo para incorporar o novo certificado. Para obter mais informações sobre como visualizar e regenerar o certificado, "[Edição de clusters](#)" consulte .



- Você pode adicionar um cluster a partir da IU da Web e a autenticação baseada em certificado é ativada automaticamente.
- Você pode adicionar um cluster por meio da CLI do Unified Manager, a autenticação baseada em certificado não está habilitada por padrão. Se você adicionar um cluster usando a CLI do Unified Manager, será necessário editar o cluster usando a IU do Unified Manager. Você pode ver "[Comandos de CLI do Unified Manager compatíveis](#)" para adicionar um cluster usando a CLI do Unified Manager.
- Se a autenticação baseada em certificado estiver ativada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurar para outro servidor do Unified Manager onde o nome de host ou o endereço IP forem alterados, o monitoramento do cluster poderá falhar. Para evitar a falha, edite e salve os detalhes do cluster. Para obter mais informações sobre como editar os detalhes do cluster, "[Edição de clusters](#)" consulte .

+

**Certificados de cluster:** Este certificado é de propriedade da ONTAP. Não é possível adicionar um cluster ao Unified Manager com um certificado expirado e, se o certificado já tiver expirado, você deve regenerá-lo antes de adicionar o cluster. Para obter informações sobre a geração de certificados, consulte o artigo da base de conhecimento (KB) "[Como renovar um certificado auto-assinado do ONTAP na interface do utilizador do System Manager](#)" .

- Você precisa ter espaço adequado no servidor do Unified Manager. Você é impedido de adicionar um cluster ao servidor quando mais de 90% de espaço no diretório do banco de dados já estiver consumido.

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

## Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração do cluster**.
2. Na página Configuração de cluster, clique em **Add**.
3. Na caixa de diálogo Adicionar cluster, especifique os valores necessários, como o nome do host ou o

endereço IP do cluster, o nome do usuário, a senha e o número da porta.

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

4. Clique em **Enviar**.
5. Na caixa de diálogo autorizar host, clique em **Exibir certificado** para exibir as informações do certificado sobre o cluster.
6. Clique em **Sim**.

Depois de salvar os detalhes do cluster, você pode ver o certificado de comunicação TLS mútua para um cluster.

Se a autenticação baseada em certificado não estiver ativada, o Unified Manager verificará o certificado somente quando o cluster for adicionado inicialmente. O Unified Manager não verifica o certificado de cada chamada de API para o ONTAP.

Depois que todos os objetos de um novo cluster forem descobertos, o Unified Manager começará a coletar dados históricos de desempenho dos 15 dias anteriores. Essas estatísticas são coletadas usando a funcionalidade de coleta de continuidade de dados. Esse recurso fornece mais de duas semanas de informações de desempenho para um cluster imediatamente após ser adicionado. Após a conclusão do ciclo de coleta de continuidade de dados, os dados de desempenho do cluster em tempo real são coletados, por padrão, a cada cinco minutos.



Como a coleta de dados de desempenho de 15 dias é intensiva em CPU, sugere-se que você alterne a adição de novos clusters para que as pesquisas de coleta de continuidade de dados não sejam executadas em muitos clusters ao mesmo tempo. Além disso, se você reiniciar o Unified Manager durante o período de coleta de continuidade de dados, a coleta será interrompida e você verá lacunas nos gráficos de desempenho para o período de tempo em falta.



Se você receber uma mensagem de erro que não pode adicionar o cluster, verifique se os relógios nos dois sistemas não estão sincronizados e a data de início do certificado HTTPS do Unified Manager é posterior à data no cluster. Você deve garantir que os relógios são sincronizados usando NTP ou um serviço similar.

## Informações relacionadas

["Instalando um certificado HTTPS assinado e retornado pela CA"](#)

## Configurando o Unified Manager para enviar notificações de alerta

Você pode configurar o Unified Manager para enviar notificações que o alertam sobre eventos no seu ambiente. Antes que as notificações possam ser enviadas, você deve configurar várias outras opções do Unified Manager.

### Antes de começar

Tem de ter a função Administrador de aplicações.

Depois de implantar o Unified Manager e concluir a configuração inicial, você deve considerar a configuração

do ambiente para acionar alertas e gerar e-mails de notificação ou traps SNMP com base no recebimento de eventos.

## Passos

### 1. "Configurar as definições de notificação de eventos".

Se você quiser que notificações de alerta sejam enviadas quando determinados eventos ocorrerem em seu ambiente, configure um servidor SMTP e forneça um endereço de e-mail a partir do qual a notificação de alerta será enviada. Se você quiser usar traps SNMP, você pode selecionar essa opção e fornecer as informações necessárias.

### 2. "Ativar autenticação remota".

Se você quiser que os usuários remotos LDAP ou ative Directory acessem a instância do Unified Manager e recebam notificações de alerta, habilite a autenticação remota.

### 3. "Adicionar servidores de autenticação".

Você pode adicionar servidores de autenticação para que usuários remotos dentro do servidor de autenticação possam acessar o Unified Manager.

### 4. "Adicionar utilizadores".

Você pode adicionar vários tipos diferentes de usuários locais ou remotos e atribuir funções específicas. Ao criar um alerta, você atribui um usuário para receber as notificações de alerta.

### 5. "Adicionar alertas".

Depois de adicionar o endereço de e-mail para enviar notificações, adicionar usuários para receber notificações, configurar as configurações de rede e configurar as opções SMTP e SNMP necessárias para o seu ambiente, você poderá atribuir alertas.

## Configurar definições de notificação de eventos

Você pode configurar o Unified Manager para enviar notificações de alerta quando um evento é gerado ou quando um evento é atribuído a um usuário. Você pode configurar o servidor SMTP que é usado para enviar o alerta, e você pode definir vários mecanismos de notificação - por exemplo, notificações de alerta podem ser enviadas como e-mails ou traps SNMP.

### Antes de começar

Você deve ter as seguintes informações:

- Endereço de e-mail a partir do qual a notificação de alerta é enviada

O endereço de e-mail aparece no campo "de" nas notificações de alerta enviadas. Se o e-mail não puder ser entregue por qualquer motivo, esse endereço de e-mail também será usado como destinatário de e-mails não entregues.

- Nome do host do servidor SMTP e nome de usuário e senha para acessar o servidor
- Nome do host ou endereço IP para o host de destino de intercetação que receberá o trap SNMP, juntamente com a versão SNMP, porta de intercetação de saída, comunidade e outros valores de configuração SNMP necessários

Para especificar vários destinos de intercetação, separe cada host com uma vírgula. Nesse caso, todas as outras configurações SNMP, como versão e porta de intercetação de saída, devem ser as mesmas para todos os hosts da lista.

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

## Passos

1. No painel de navegação esquerdo, clique em **Geral > notificações**.
2. Na página notificações, configure as configurações apropriadas.

### Notas:

- Se o endereço de e-mail for pré-preenchido com o endereço "[ActiveIQUnifiedManager@localhost.com](mailto:ActiveIQUnifiedManager@localhost.com)", você deve alterá-lo para um endereço de e-mail real e funcional para garantir que todas as notificações de e-mail sejam entregues com sucesso.
  - Se o nome do host do servidor SMTP não puder ser resolvido, você poderá especificar o endereço IP (IPv4 ou IPv6) do servidor SMTP em vez do nome do host.
3. Clique em **Salvar**.
  4. Se você tiver selecionado a opção **Use STARTTLS** ou **Use SSL**, uma página de certificado será exibida após clicar no botão **Save**. Verifique os detalhes do certificado e aceite o certificado para salvar as configurações de notificação.

Você pode clicar no botão **Exibir detalhes do certificado** para exibir os detalhes do certificado. Se o certificado existente estiver expirado, desmarque a caixa **usar STARTTLS** ou **usar SSL**, salve as configurações de notificação e marque novamente a caixa **usar STARTTLS** ou **usar SSL** para exibir um novo certificado.

## Ativar autenticação remota

Você pode habilitar a autenticação remota para que o servidor do Unified Manager possa se comunicar com seus servidores de autenticação. Os usuários do servidor de autenticação podem acessar a interface gráfica do Unified Manager para gerenciar objetos e dados de storage.

### Antes de começar

Tem de ter a função Administrador de aplicações.



O servidor do Unified Manager deve estar conectado diretamente ao servidor de autenticação. Você deve desativar quaisquer clientes LDAP locais, como SSSD (System Security Services Daemon) ou NSLCD (Name Service LDAP Caching Daemon).

Você pode ativar a autenticação remota usando LDAP aberto ou ative Directory. Se a autenticação remota estiver desativada, os usuários remotos não poderão acessar o Unified Manager.

A autenticação remota é suportada por LDAP e LDAPS (Secure LDAP). O Unified Manager usa o 389 como a porta padrão para comunicação não segura e o 636 como a porta padrão para comunicação segura.



O certificado usado para autenticar usuários deve estar em conformidade com o formato X.509.

## Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação remota**.
2. Marque a caixa **Ativar autenticação remota...**
3. No campo Serviço de autenticação, selecione o tipo de serviço e configure o serviço de autenticação.

Para tipo de autenticação...	Digite as seguintes informações...
Ative Directory	<ul style="list-style-type: none"> <li>• Nome do administrador do servidor de autenticação em um dos seguintes formatos: <ul style="list-style-type: none"> <li>◦ domainname\username</li> <li>◦ username@domainname</li> <li>◦ Bind Distinguished Name (Usando a notação LDAP apropriada)</li> </ul> </li> <li>• Senha do administrador</li> <li>• Nome diferenciado base (usando a notação LDAP apropriada)</li> </ul>
Abra o LDAP	<ul style="list-style-type: none"> <li>• Vincular nome distinto (na notação LDAP apropriada)</li> <li>• Vincular senha</li> <li>• Nome diferenciado da base</li> </ul>

Se a autenticação de um usuário do active Directory demorar muito tempo ou tempo limite, o servidor de autenticação provavelmente levará muito tempo para responder. Desativar o suporte para grupos aninhados no Unified Manager pode reduzir o tempo de autenticação.

Se você selecionar a opção usar conexão segura para o servidor de autenticação, o Unified Manager se comunicará com o servidor de autenticação usando o protocolo SSL (Secure Sockets Layer).

4. **Opcional:** Adicione servidores de autenticação e teste a autenticação.
5. Clique em **Salvar**.

### Desativando grupos aninhados da autenticação remota

Se a autenticação remota estiver ativada, você poderá desativar a autenticação de grupo aninhado para que somente usuários individuais, e não membros de grupo, possam se autenticar remotamente no Unified Manager. Você pode desativar grupos aninhados quando quiser melhorar o tempo de resposta de autenticação do active Directory.

#### Antes de começar

- Tem de ter a função Administrador de aplicações.
- A desativação de grupos aninhados só é aplicável ao usar o active Directory.

Desativar o suporte para grupos aninhados no Unified Manager pode reduzir o tempo de autenticação. Se o suporte a grupos aninhados estiver desativado e se um grupo remoto for adicionado ao Unified Manager, os usuários individuais deverão ser membros do grupo remoto para se autenticar no Unified Manager.

#### Passos



1. No painel de navegação esquerdo, clique em **Geral > Autenticação remota**.
2. Marque a caixa **Desativar Pesquisa de grupos aninhados**.
3. Clique em **Salvar**.

## Configurando serviços de autenticação

Os serviços de autenticação permitem a autenticação de usuários remotos ou grupos remotos em um servidor de autenticação antes de fornecer acesso ao Unified Manager. Você pode autenticar usuários usando serviços de autenticação predefinidos (como Active Directory ou OpenLDAP) ou configurando seu próprio mecanismo de autenticação.

### Antes de começar

- Tem de ter ativado a autenticação remota.
- Tem de ter a função Administrador de aplicações.

### Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação remota**.
2. Selecione um dos seguintes serviços de autenticação:

Se selecionar...	Então faça isso...
Active Directory	<p>a. Introduza o nome e a palavra-passe do administrador.</p> <p>b. Especifique o nome distinto base do servidor de autenticação.</p> <p>Por exemplo, se o nome de domínio do servidor de autenticação for mais de <a href="#">ou@domain.com</a>, então o nome distinto base é</p>
OpenLDAP	<p>a. Introduza o nome distinto de ligação e a palavra-passe de ligação.</p> <p>b. Especifique o nome distinto base do servidor de autenticação.</p> <p>Por exemplo, se o nome de domínio do servidor de autenticação for mais de <a href="#">ou@domain.com</a>, então o nome distinto base é</p>

Se selecionar...	Então faça isso...
Outros	<p>a. Introduza o nome distinto de ligação e a palavra-passe de ligação.</p> <p>b. Especifique o nome distinto base do servidor de autenticação.</p> <p>Por exemplo, se o nome de domínio do servidor de autenticação for mais de <code>ou@domain.com</code>, então o nome distinto base é</p> <p>c. Especifique a versão do protocolo LDAP suportada pelo servidor de autenticação.</p> <p>d. Introduza o nome de utilizador, a associação ao grupo, o grupo de utilizadores e os atributos de membro.</p>



Se você quiser modificar o serviço de autenticação, você deve excluir quaisquer servidores de autenticação existentes e adicionar novos servidores de autenticação.

3. Clique em **Salvar**.

### Adicionando servidores de autenticação

Você pode adicionar servidores de autenticação e ativar a autenticação remota no servidor de gerenciamento para que os usuários remotos no servidor de autenticação possam acessar o Unified Manager.


#### Antes de começar

- As seguintes informações devem estar disponíveis:
  - Nome do host ou endereço IP do servidor de autenticação
  - Número da porta do servidor de autenticação
- Você deve ter habilitado a autenticação remota e configurado o serviço de autenticação para que o servidor de gerenciamento possa autenticar usuários remotos ou grupos no servidor de autenticação.
- Tem de ter a função Administrador de aplicações.

Se o servidor de autenticação que você está adicionando fizer parte de um par de alta disponibilidade (HA) (usando o mesmo banco de dados), você também poderá adicionar o servidor de autenticação de parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação está inacessível.

#### Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação remota**.
2. Ative ou desative a opção **Use secure Connection**:

Se você quiser...	Então faça isso...
Ative-o.	<p>a. Selecione a opção <b>usar conexão segura</b>.</p> <p>b. Na área servidores de autenticação, clique em <b>Adicionar</b>.</p> <p>c. Na caixa de diálogo Adicionar servidor de autenticação, insira o nome de autenticação ou o endereço IP (IPv4 ou IPv6) do servidor.</p> <p>d. Na caixa de diálogo autorizar host, clique em Exibir certificado.</p> <p>e. Na caixa de diálogo Exibir certificado, verifique as informações do certificado e clique em <b>Fechar</b>.</p> <p>f. Na caixa de diálogo autorizar Host, clique em <b>Yes</b>.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Quando você ativa a opção <b>Use Secure Connection Authentication</b>, o Unified Manager se comunica com o servidor de autenticação e exibe o certificado. O Unified Manager usa o 636 como porta padrão para comunicação segura e o número de porta 389 para comunicação não segura.</p> </div>
Desative-o.	<p>a. Desmarque a opção <b>Use Secure Connection</b>.</p> <p>b. Na área servidores de autenticação, clique em <b>Adicionar</b>.</p> <p>c. Na caixa de diálogo Adicionar servidor de autenticação, especifique o nome do host ou o endereço IP (IPv4 ou IPv6) do servidor e os detalhes da porta.</p> <p>d. Clique em <b>Add</b>.</p>

O servidor de autenticação adicionado é exibido na área servidores.

- Execute uma autenticação de teste para confirmar que é possível autenticar usuários no servidor de autenticação que você adicionou.

### Testando a configuração dos servidores de autenticação

Você pode validar a configuração de seus servidores de autenticação para garantir que o servidor de gerenciamento seja capaz de se comunicar com eles. É possível validar a configuração pesquisando um usuário remoto ou grupo remoto de seus servidores de autenticação e autenticando-os usando as configurações configuradas.

## Antes de começar

- Você deve ter habilitado a autenticação remota e configurado o serviço de autenticação para que o servidor do Unified Manager possa autenticar o usuário remoto ou o grupo remoto.
- Você deve ter adicionado seus servidores de autenticação para que o servidor de gerenciamento possa pesquisar o usuário remoto ou grupo remoto desses servidores e autenticá-los.
- Tem de ter a função Administrador de aplicações.

Se o serviço de autenticação estiver definido como ativo Directory e se você estiver validando a autenticação de usuários remotos que pertencem ao grupo principal do servidor de autenticação, as informações sobre o grupo principal não serão exibidas nos resultados de autenticação.

## Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação remota**.
2. Clique em **Test Authentication**.
3. Na caixa de diálogo testar usuário, especifique o nome de usuário e a senha do usuário remoto ou o nome de usuário do grupo remoto e clique em **Teste**.

Se estiver a autenticar um grupo remoto, não deve introduzir a palavra-passe.

## 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 Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento é gerado.
- Você deve saber os recursos e eventos para os quais deseja acionar o alerta e os nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se você quiser que um script seja executado com base no evento, você deve ter adicionado o script ao Unified Manager usando a página Scripts.
- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

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

## Passos

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

Você pode definir um filtro especificando uma cadeia de texto no campo **Name contains** para selecionar um grupo de recursos. Com base na cadeia de texto especificada, a lista de recursos disponíveis exibe

apenas os recursos que correspondem à regra de filtro. A cadeia de texto especificada é sensível a maiúsculas e minúsculas.

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

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



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

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



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

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

7. Clique em **Salvar**.

#### Exemplo de adição de um alerta

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

- Nome do alerta: HealthTest
- Recursos: Inclui todos os volumes cujo nome contém "abc" e exclui todos os volumes cujo nome contém "xyz"
- Eventos: Inclui todos os eventos críticos de saúde
- Ações: Inclui "[sample@domain.com](mailto:sample@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:

#### Passos

1. Clique em **Nome** e insira **Teste de integridade** no campo **Nome do alerta**.
2. Clique em **recursos** e, na guia incluir, selecione **volumes** na lista suspensa.
  - a. Digite **abc** no campo **Nome contém** para exibir os volumes cujo nome contém "'abc'".
  - b. Selecione **\*[All Volumes whose name contains 'abc']** na área recursos disponíveis e mova-o para a área recursos selecionados.
  - c. Clique em **Excluir**, digite **xyz** no 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 digite **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**.

## Alterar a palavra-passe do utilizador local

Você pode alterar sua senha de login de usuário local para evitar possíveis riscos de segurança.

### Antes de começar

Você deve estar conectado como um usuário local.

As senhas para o usuário de manutenção e para usuários remotos não podem ser alteradas usando estas etapas. Para alterar uma palavra-passe de utilizador remoto, contacte o administrador da palavra-passe. Para alterar a senha do usuário de manutenção, "[Utilizar a consola de manutenção](#)" consulte .

### Passos

1. Faça login no Unified Manager.
2. Na barra de menu superior, clique no ícone do usuário e, em seguida, clique em **alterar senha**.

A opção **alterar senha** não será exibida se você for um usuário remoto.

3. Na caixa de diálogo alterar senha, insira a senha atual e a nova senha.
4. Clique em **Salvar**.

Se o Unified Manager estiver configurado em uma configuração de alta disponibilidade, você deverá alterar a senha no segundo nó da configuração. Ambas as instâncias devem ter a mesma senha.

## Definir o tempo limite de inatividade da sessão

Você pode especificar o valor de tempo limite de inatividade do Unified Manager para que a sessão seja encerrada automaticamente após um determinado período de tempo. Por padrão, o tempo limite é definido para 4.320 minutos (72 horas).

### Antes de começar

Tem de ter a função Administrador de aplicações.

Esta definição afeta todas as sessões de utilizador com sessão iniciada.



Essa opção não estará disponível se você tiver habilitado a autenticação SAML (Security Assertion Markup Language).

### Passos

1. No painel de navegação à esquerda, clique em **Geral > Definições da funcionalidade**.

2. Na página **Configurações de recursos**, especifique o tempo limite de inatividade escolhendo uma das seguintes opções:

Se você quiser...	Então faça isso...
Não tenha tempo limite definido para que a sessão nunca seja fechada automaticamente	No painel <b>tempo limite de inatividade</b> , mova o botão deslizante para a esquerda (Desligado) e clique em <b>aplicar</b> .
Defina um número específico de minutos como o valor de tempo limite	No painel <b>tempo limite de inatividade</b> , mova o botão deslizante para a direita (ligado), especifique o valor de tempo limite de inatividade em minutos e clique em <b>aplicar</b> .

## Alterando o nome do host do Unified Manager

Em algum momento, talvez você queira alterar o nome do host do sistema no qual você instalou o Unified Manager. Por exemplo, você pode querer renomear o host para identificar mais facilmente seus servidores do Unified Manager por tipo, grupo de trabalho ou grupo de cluster monitorado.

As etapas necessárias para alterar o nome do host são diferentes dependendo se o Unified Manager está sendo executado em um servidor VMware ESXi, em um servidor Red Hat Linux ou em um servidor Microsoft Windows.

### Alterando o nome do host do dispositivo virtual do Unified Manager

O host de rede recebe um nome quando o dispositivo virtual do Unified Manager é implantado pela primeira vez. Você pode alterar o nome do host após a implantação. Se você alterar o nome do host, você também deve regenerar o certificado HTTPS.

#### Antes de começar

Você deve estar conectado ao Unified Manager como usuário de manutenção ou ter a função Administrador de aplicativos atribuída a você para executar essas tarefas.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a IU da Web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, então você teria designado um nome para o host de rede. Se você configurou a rede usando DHCP, o nome do host deve ser retirado do DNS. Se o DHCP ou DNS não estiver configurado corretamente, o nome do host "Unified Manager" será atribuído automaticamente e associado ao certificado de segurança.

Independentemente de como o nome do host foi atribuído, se você alterar o nome do host e pretender usar o novo nome do host para acessar a IU da Web do Unified Manager, será necessário gerar um novo certificado de segurança.

Se você acessar a IU da Web usando o endereço IP do servidor em vez do nome do host, não será necessário gerar um novo certificado se você alterar o nome do host. No entanto, é a melhor prática atualizar o certificado para que o nome do host no certificado corresponda ao nome do host real.

Se você alterar o nome do host no Unified Manager, será necessário atualizar manualmente o nome do host no OnCommand Workflow Automation (WFA). O nome do host não é atualizado automaticamente no WFA.

O novo certificado não entrará em vigor até que a máquina virtual do Unified Manager seja reinicializada.

## Passos

### 1. Gerar um certificado de segurança HTTPS

Se você quiser usar o novo nome de host para acessar a IU da Web do Unified Manager, será necessário regenerar o certificado HTTPS para associá-lo ao novo nome de host.

### 2. Reinicie a máquina virtual do Unified Manager

Depois de regenerar o certificado HTTPS, você deve reiniciar a máquina virtual do Unified Manager.

## Gerando um certificado de segurança HTTPS

Quando o Active IQ Unified Manager é instalado pela primeira vez, um certificado HTTPS padrão é instalado. Você pode gerar um novo certificado de segurança HTTPS que substitui o certificado existente.

### Antes de começar

Tem de ter a função Administrador de aplicações.

Pode haver vários motivos para regenerar o certificado, como se você quiser ter melhores valores para Nome distinto (DN) ou se quiser um tamanho de chave maior, ou um período de validade mais longo ou se o certificado atual expirou.

Se você não tiver acesso à IU da Web do Unified Manager, poderá regenerar o certificado HTTPS com os mesmos valores usando o console de manutenção. Ao regenerar certificados, você pode definir o tamanho da chave e a duração da validade da chave. Se você usar a `Reset Server Certificate` opção do console de manutenção, um novo certificado HTTPS será criado, válido por 397 dias. Este certificado terá uma chave RSA de tamanho 2048 bits.

## Passos

1. No painel de navegação esquerdo, clique em **Geral > certificado HTTPS**.
2. Clique em **Regenerate HTTPS Certificate**.

A caixa de diálogo Reperate HTTPS Certificate (regenerar certificado HTTPS) é exibida.

3. Selecione uma das opções a seguir, dependendo de como você deseja gerar o certificado:

Se você quiser...	Faça isso...
Regenere o certificado com os valores atuais	Clique na opção <b>Regenerate usando atributos de certificado atuais</b> .



Se você quiser...	Faça isso...
Gerar o certificado usando valores diferentes	<p data-bbox="842 159 1380 222">Clique na opção <b>Atualizar os atributos de certificado atuais</b>.</p> <p data-bbox="842 260 1484 632">Os campos Nome Comum e nomes alternativos usarão os valores do certificado existente se você não inserir novos valores. O "Nome Comum" deve ser definido como o FQDN do host. Os outros campos não exigem valores, mas você pode inserir valores, por exemplo, para o E-MAil, EMPRESA, DEPARTAMENTO, cidade, estado e país, se quiser que esses valores sejam preenchidos no certificado. Você também pode selecionar a partir do TAMANHO DA CHAVE disponível (o algoritmo da chave é "RSA".) e PERÍODO DE validade.</p> <ul data-bbox="1015 680 1435 898" style="list-style-type: none"> <li data-bbox="1015 680 1435 779">• Os valores permitidos para o tamanho da chave são 2048, 3072 e 4096.</li> <li data-bbox="1015 804 1435 898">• Os períodos de validade são de no mínimo 1 dia a no máximo 36500 dias.</li> </ul> <p data-bbox="1036 936 1451 1409">Embora seja permitido um período de validade de 36500 dias, recomenda-se que você use um período de validade não superior a 397 dias ou 13 meses. Porque se você selecionar um período de validade superior a 397 dias e Planejar exportar um CSR para este certificado e assiná-lo por uma CA bem conhecida, a validade do certificado assinado devolvido a você pela CA será reduzida para 397 dias.</p> <ul data-bbox="1015 1451 1451 1923" style="list-style-type: none"> <li data-bbox="1015 1451 1451 1923">• Você pode selecionar a caixa de seleção "Excluir informações de identificação local (por exemplo, localhost)" se quiser remover as informações de identificação local do campo nomes alternativos no certificado. Quando esta caixa de verificação está selecionada, apenas o que introduzir no campo é utilizado no campo nomes alternativos. Quando deixado em branco, o certificado resultante não terá um campo de nomes alternativos.</li> </ul>

4. Clique em **Yes** para regenerar o certificado.
5. Reinicie o servidor do Unified Manager para que o novo certificado entre em vigor.
6. Verifique as novas informações do certificado visualizando o certificado HTTPS.

### Reiniciando a máquina virtual do Unified Manager

Você pode reiniciar a máquina virtual a partir do console de manutenção do Unified Manager. Você deve reiniciar depois de gerar um novo certificado de segurança ou se houver um problema com a máquina virtual.

#### Antes de começar

O dispositivo virtual está ligado.

Você está conectado ao console de manutenção como usuário de manutenção.

Você também pode reiniciar a máquina virtual do vSphere usando a opção **Restart Guest**. Consulte a documentação da VMware para obter mais informações.

#### Passos

1. Acesse à consola de manutenção.
2. Selecione **Configuração do sistema > Reiniciar Máquina Virtual**.

### Alteração do nome de host do Unified Manager em sistemas Linux

Em algum momento, você pode querer alterar o nome do host da máquina Red Hat Enterprise Linux na qual você instalou o Unified Manager. Por exemplo, você pode querer renomear o host para identificar mais facilmente seus servidores do Unified Manager por tipo, grupo de trabalho ou grupo de cluster monitorado quando você listar suas máquinas Linux.

#### Antes de começar

Você deve ter acesso de usuário raiz ao sistema Linux no qual o Unified Manager está instalado.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a IU da Web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, então você teria designado um nome para o host de rede. Se você configurou a rede usando DHCP, o nome do host deve ser retirado do servidor DNS.

Independentemente de como o nome do host foi atribuído, se você alterar o nome do host e pretender usar o novo nome do host para acessar a IU da Web do Unified Manager, será necessário gerar um novo certificado de segurança.

Se você acessar a IU da Web usando o endereço IP do servidor em vez do nome do host, não será necessário gerar um novo certificado se você alterar o nome do host. No entanto, é a melhor prática atualizar o certificado, de modo que o nome do host no certificado corresponda ao nome do host real. O novo certificado não entra em vigor até que a máquina Linux seja reiniciada.

Se você alterar o nome do host no Unified Manager, será necessário atualizar manualmente o nome do host no OnCommand Workflow Automation (WFA). O nome do host não é atualizado automaticamente no WFA.

#### Passos

1. Faça login como usuário raiz no sistema Unified Manager que você deseja modificar.
2. Pare o software Unified Manager e o software MySQL associado digitando o seguinte comando:

```
systemctl stop ocieau ocie mysqld
```

3. Altere o nome do host usando o comando Linux hostnamectl:

```
hostnamectl set-hostname new_FQDN
```

```
hostnamectl set-hostname nuhost.corp.widget.com
```

4. Regenere o certificado HTTPS para o servidor:

```
/opt/netapp/essentials/bin/cert.sh create
```

5. Reinicie o serviço de rede:

```
systemctl restart NetworkManager.service
```

6. Depois que o serviço for reiniciado, verifique se o novo nome de host é capaz de fazer ping em si mesmo:

```
ping new_hostname
```

```
ping nuhost
```

Este comando deve retornar o mesmo endereço IP que foi definido anteriormente para o nome original do host.

7. Após concluir e verificar a alteração do nome do host, reinicie o Unified Manager digitando o seguinte comando:

```
systemctl start mysqld ocie ocieau
```

## Ativar e desativar o gerenciamento de armazenamento baseado em políticas

A partir do Unified Manager 9,7, você pode provisionar workloads de storage (volumes e LUNs) nos clusters do ONTAP e gerenciar esses workloads com base em níveis de serviço de performance atribuídos. Essa funcionalidade é semelhante à criação de workloads no ONTAP System Manager e à inclusão de políticas de QoS, mas, quando aplicada usando o Unified Manager, você pode provisionar e gerenciar workloads em todos os clusters que sua instância do Unified Manager está monitorando.

Tem de ter a função Administrador de aplicações.

Essa opção está ativada por padrão, mas você pode desativá-la se não quiser provisionar e gerenciar cargas de trabalho usando o Unified Manager.

Quando ativada, esta opção fornece muitos itens novos na interface do utilizador:

Novo conteúdo	Localização
Uma página para provisionar novos workloads	Disponível em <b>Common Tasks &gt; Provisioning</b>
Uma página para criar políticas de nível de serviço de desempenho	Disponível a partir de <b>Definições &gt; políticas &gt; níveis de Serviço de desempenho</b>
Uma página para criar políticas de eficiência de storage de performance	Disponível a partir de <b>Definições &gt; políticas &gt; eficiência de armazenamento</b>
Painéis que descrevem o desempenho atual de workload e o IOPS de workload	Disponível a partir do Dashboard

Consulte a ajuda on-line do produto para obter mais informações sobre essas páginas e sobre essa funcionalidade.

### Passos

1. No painel de navegação à esquerda, clique em **Geral > Definições da funcionalidade**.
2. Na página **Configurações de recursos**, desative ou ative o gerenciamento de armazenamento baseado em políticas escolhendo uma das seguintes opções:

Se você quiser...	Então faça isso...
Desative o gerenciamento de storage baseado em políticas	No painel <b>Gerenciamento de armazenamento baseado em políticas</b> , mova o botão deslizante para a esquerda.
Habilite o gerenciamento de storage baseado em políticas	No painel <b>Gerenciamento de armazenamento baseado em políticas</b> , mova o botão deslizante para a direita.

## Configuração do backup do Unified Manager

Você pode configurar o recurso de backup no Unified Manager por meio de um conjunto de etapas de configuração a serem executadas nos sistemas host e no console de manutenção por meio.

Para obter informações sobre as etapas de configuração, "[Gerenciamento de operações de backup e restauração](#)" consulte .

## Gerir definições de funcionalidades

A página Configurações de recursos permite ativar e desativar recursos específicos no Active IQ Unified Manager. Isso inclui criar e gerenciar objetos de armazenamento com base em políticas, ativar o gateway de API e o banner de login, fazer upload de scripts para gerenciar alertas, agendar uma sessão de IU da Web com base no tempo de inatividade e desativar o recebimento de eventos da plataforma Active IQ.



A página Configurações de recursos só está disponível para usuários com função Administrador de aplicativos.

Para obter informações sobre o carregamento de scripts, ["Ativar e desativar o carregamento de scripts"](#) consulte .

## Habilitando o gerenciamento de storage baseado em políticas

A opção **Gerenciamento de armazenamento baseado em políticas** permite o gerenciamento de armazenamento com base nos objetivos de nível de serviço (SLOs). Esta opção está ativada por predefinição.

Ao ativar esse recurso, você pode provisionar workloads de storage nos clusters do ONTAP adicionados à sua instância do Active IQ Unified Manager e gerenciar esses workloads com base nos níveis de Serviço de desempenho atribuídos e nas políticas de eficiência de storage.

Pode optar por ativar ou desativar esta funcionalidade a partir de **Geral > Definições de funcionalidade > Gestão de armazenamento baseada em políticas**. Ao ativar este recurso, as seguintes páginas estão disponíveis para operação e monitoramento:

- Provisionamento (provisionamento de workload de storage)
- **Políticas > níveis de Serviço de desempenho**
- **Políticas > eficiência de armazenamento**
- Coluna cargas de trabalho gerenciadas pela coluna Performance Service Level (nível de Serviço de Performance) na página clusters Setup (Configuração dos clusters)
- Painel desempenho da carga de trabalho no **Dashboard**

Você pode usar as telas para criar níveis de Serviço de Performance e políticas de eficiência de storage e provisionar workloads de storage. Também é possível monitorar os workloads de storage que estão em conformidade com os níveis de Serviço de performance atribuídos e os que não estão em conformidade. O painel Performance de workload e Workload IOPS também permite avaliar a capacidade e a performance (IOPS) totais, disponíveis e usadas dos clusters no data center com base nos workloads de storage provisionados neles.

Depois de ativar esse recurso, você pode executar as APIs REST do Unified Manager para executar algumas dessas funções da categoria **barra de menus > botão Ajuda > Documentação da API > provedor de armazenamento**. Como alternativa, você pode inserir o nome do host ou o endereço IP e o URL para acessar a página da API REST no formato `.https://<hostname>/docs/api/`

Para obter mais informações sobre as APIs, ["Primeiros passos com as APIs REST do Active IQ Unified Manager"](#) consulte .

## Ativando o API Gateway

O recurso API Gateway permite que o Active IQ Unified Manager seja um único plano de controle a partir do qual você pode gerenciar vários clusters ONTAP, sem fazer login neles individualmente.

Você pode habilitar esse recurso nas páginas de configuração que aparecem quando você faz login no Unified Manager pela primeira vez. Alternativamente, você pode ativar ou desativar esse recurso de **Geral > Configurações de recursos > Gateway API**.

As APIs REST do Unified Manager são diferentes das APIs REST do ONTAP, e nem todas as funcionalidades das APIs REST do ONTAP podem ser aproveitadas com as APIs REST do Unified Manager. No entanto, se você tiver um requisito comercial específico para acessar as APIs do ONTAP para gerenciar recursos específicos que não sejam expostos ao Gerenciador Unificado, poderá ativar o recurso de gateway de API e executar as APIs do ONTAP. O gateway atua como um proxy para túnel as solicitações de API, mantendo as solicitações de cabeçalho e corpo no mesmo formato que nas APIs do ONTAP. Você pode usar suas credenciais do Unified Manager e executar APIs específicas para acessar e gerenciar os clusters do ONTAP sem passar credenciais de cluster individuais. O Unified Manager funciona como um ponto único de gerenciamento para executar as APIs nos clusters do ONTAP gerenciados pela sua instância do Unified Manager. A resposta retornada pelas APIs é a mesma que a resposta retornada pelas respectivas APIs REST do ONTAP executadas diretamente do ONTAP.

Depois de ativar esse recurso, você pode executar as APIs REST do Unified Manager a partir da categoria **barra de menus > botão Ajuda > Documentação da API > gateway**. Como alternativa, você pode inserir o nome do host ou o endereço IP e o URL para acessar a página REST API no formato

<https://<hostname>/docs/api/>

Para obter mais informações sobre as APIs, "[Primeiros passos com as APIs REST do Active IQ Unified Manager](#)" consulte .

## Especificar o tempo limite de inatividade

Você pode especificar o valor de tempo limite de inatividade para o Active IQ Unified Manager. Após uma inatividade do tempo especificado, o aplicativo é desconectado automaticamente. Esta opção está ativada por predefinição.

Pode desativar esta funcionalidade ou modificar a hora a partir de **Geral > Definições da funcionalidade > tempo limite de inatividade**. Depois de ativar este recurso, você deve especificar o limite de tempo de inatividade (em minutos) no campo **LOGOUT AFTER**, após o qual o sistema faz logout automaticamente. O valor padrão é de 4320 minutos (72 horas).



Essa opção não estará disponível se você tiver habilitado a autenticação SAML (Security Assertion Markup Language).

## Ativar eventos do portal Active IQ

Você pode especificar se deseja ativar ou desativar eventos do portal Active IQ. Essa configuração permite que o portal do Active IQ descubra e exiba eventos adicionais sobre configuração do sistema, cabeamento e assim por diante. Esta opção está ativada por predefinição.

Ao ativar esse recurso, o Active IQ Unified Manager exibe eventos descobertos pelo portal do Active IQ. Esses eventos são criados executando um conjunto de regras contra as mensagens do AutoSupport geradas a partir de todos os sistemas de armazenamento monitorados. Esses eventos são diferentes dos outros eventos do Unified Manager e identificam incidentes ou riscos relacionados à configuração do sistema, cabeamento, práticas recomendadas e problemas de disponibilidade.

Pode optar por ativar ou desativar esta funcionalidade a partir de **Geral > Definições da funcionalidade > Eventos do Portal Active IQ**. Em sites sem acesso à rede externa, você deve carregar as regras manualmente de **Gerenciamento de armazenamento > Configuração do evento > regras de upload**.

Esta funcionalidade está ativada por predefinição. A desativação desse recurso impede que os eventos do

Active IQ sejam descobertos ou exibidos no Gerenciador Unificado. Quando desativado, a ativação desse recurso permite que o Gerenciador Unificado receba os eventos do Active IQ em um cluster em um horário predefinido de 00:15 para esse fuso horário do cluster.

## Ativar e desativar as definições de segurança para conformidade

Usando o botão **Personalizar** no painel **Painel de Segurança** da página Configurações de recursos, você pode ativar ou desativar os parâmetros de segurança para monitoramento de conformidade no Unified Manager.

As configurações habilitadas ou desativadas nesta página regem o status geral de conformidade dos clusters e das VMs de armazenamento no Unified Manager. Com base nas seleções, as colunas correspondentes são visíveis na visualização **Segurança: Todos os clusters** da página de inventário dos clusters e na visualização **Segurança: Todas as VMs de armazenamento** da página de inventário das VMs de armazenamento.



Somente usuários com função de administrador podem editar essas configurações.

Os critérios de segurança dos clusters do ONTAP, das máquinas virtuais de storage e dos volumes são avaliados em relação às recomendações definidas no "[Guia de endurecimento de segurança para NetApp ONTAP 9](#)". O painel Segurança no painel e na página Segurança exibe o status padrão de conformidade de segurança dos clusters, VMs de armazenamento e volumes. Os eventos de segurança também são gerados e as ações de gerenciamento habilitadas para os clusters e as VMs de storage que têm violações de segurança.

## Personalizar as definições de segurança

Para personalizar as configurações de monitoramento de conformidade, conforme aplicável ao seu ambiente ONTAP, siga estas etapas:

### Passos

1. Clique em **Geral > Definições de funcionalidades > Painel de segurança > Personalizar**. A janela pop-up **Personalizar definições do painel de segurança** é apresentada.



Os parâmetros de conformidade de segurança que você ativa ou desativa podem afetar diretamente as exibições de segurança padrão, os relatórios e os relatórios programados nas telas clusters e VMs de armazenamento. Se você tiver carregado um relatório do excel a partir dessas telas antes de modificar os parâmetros de segurança, os relatórios do excel baixados podem estar com defeito.

2. Para ativar ou desativar as configurações personalizadas para os clusters do ONTAP, selecione a configuração geral necessária em **Cluster**. Para obter informações sobre as opções de personalização da conformidade do cluster, "[Categorias de conformidade de cluster](#)" consulte .
3. Para ativar ou desativar as configurações personalizadas para as VMs de armazenamento, selecione a configuração geral necessária em **Storage VM**. Para obter informações sobre as opções de personalização da conformidade da VM de storage, "[Categorias de conformidade de VM de storage](#)" consulte .

## Personalizar as definições de AutoSupport e autenticação

Na seção **Configurações AutoSupport**, você pode especificar se o transporte HTTPS deve ser usado para enviar mensagens AutoSupport do ONTAP.

Na seção **Configurações de autenticação**, você pode habilitar alertas do Gerenciador Unificado para o

## Ativar e desativar o carregamento de scripts

A capacidade de carregar scripts para o Unified Manager e executá-los é ativada por padrão. Se a sua organização não quiser permitir esta atividade por motivos de segurança, pode desativar esta funcionalidade.

### Antes de começar

Tem de ter a função Administrador de aplicações.

### Passos

1. No painel de navegação à esquerda, clique em **Geral > Definições da funcionalidade**.
2. Na página **Configurações de recursos**, desative ou habilite o script escolhendo uma das seguintes opções:

Se você quiser...	Então faça isso...
Desativar scripts	No painel <b>Script Upload</b> , mova o botão deslizante para a esquerda.
Ativar scripts	No painel <b>Script Upload</b> , mova o botão deslizante para a direita.

## Adicionando banner de login

Adicionar um banner de login permite que sua organização exiba qualquer informação, como, quem tem permissão de acesso ao sistema e os termos e condições de uso durante o login e logout.

Qualquer usuário, como operadores de armazenamento ou administradores, pode visualizar este banner pop-up de login durante o login, logout e tempo limite da sessão.

## Utilizar a consola de manutenção

Você pode usar o console de manutenção para configurar as configurações de rede, configurar e gerenciar o sistema no qual o Unified Manager está instalado e executar outras tarefas de manutenção que ajudam a prevenir e solucionar possíveis problemas.

### Que funcionalidade o console de manutenção fornece

O console de manutenção do Unified Manager permite que você mantenha as configurações no sistema do Unified Manager e faça as alterações necessárias para evitar que problemas ocorram.

Dependendo do sistema operacional no qual você instalou o Unified Manager, o console de manutenção



fornece as seguintes funções:

- Solucione problemas com o dispositivo virtual, especialmente se a interface da Web do Unified Manager não estiver disponível
- Atualize para versões mais recentes do Unified Manager
- Gere pacotes de suporte para enviar ao suporte técnico
- Configure as definições de rede
- Altere a palavra-passe do utilizador de manutenção
- Conecte-se a um provedor de dados externo para enviar estatísticas de desempenho
- Alterar a coleta de dados de desempenho interna
- Restaure o banco de dados e as configurações do Unified Manager a partir de uma versão com backup anterior.

## O que o utilizador de manutenção faz

O usuário de manutenção é criado durante a instalação do Unified Manager em um sistema Red Hat Enterprise Linux. O nome de usuário de manutenção é o usuário "umadmin". O usuário de manutenção tem a função Administrador do aplicativo na IU da Web e esse usuário pode criar usuários subsequentes e atribuir-lhes funções.

O usuário de manutenção, ou usuário umadmin, também pode acessar o console de manutenção do Unified Manager.

## Capacidades do utilizador de diagnóstico

O objetivo do acesso ao diagnóstico é habilitar o suporte técnico para ajudá-lo na solução de problemas e você só deve usá-lo quando direcionado pelo suporte técnico.

O usuário de diagnóstico pode executar comandos no nível do SO quando dirigido pelo suporte técnico, para fins de solução de problemas.

## Aceder à consola de manutenção

Se a interface de usuário do Unified Manager não estiver em operação ou se for necessário executar funções que não estejam disponíveis na interface do usuário, você poderá acessar o console de manutenção para gerenciar o sistema do Unified Manager.

### Antes de começar

Você precisa ter instalado e configurado o Unified Manager.

Após 15 minutos de inatividade, o console de manutenção faz o logout.



Quando instalado no VMware, se você já fez login como usuário de manutenção pelo console VMware, não será possível fazer login simultaneamente usando o Secure Shell.

### Passo

1. Siga estas etapas para acessar o console de manutenção:

Neste sistema operativo...	Siga estes passos...
VMware	<ul style="list-style-type: none"> <li>a. Usando o Secure Shell, conete-se ao endereço IP ou ao nome de domínio totalmente qualificado do dispositivo virtual do Unified Manager.</li> <li>b. Inicie sessão na consola de manutenção utilizando o nome de utilizador e a palavra-passe de manutenção.</li> </ul>
Linux	<ul style="list-style-type: none"> <li>a. Usando o Secure Shell, conete-se ao endereço IP ou ao nome de domínio totalmente qualificado do sistema Unified Manager.</li> <li>b. Inicie sessão no sistema com o nome e a palavra-passe do utilizador de manutenção (umadmin).</li> <li>c. Digite o comando <code>maintenance_console</code> e pressione Enter.</li> </ul>
Windows	<ul style="list-style-type: none"> <li>a. Faça login no sistema Unified Manager com credenciais de administrador.</li> <li>b. Inicie o PowerShell como administrador do Windows.</li> <li>c. Digite o comando <code>maintenance_console</code> e pressione Enter.</li> </ul>

O menu do console de manutenção do Unified Manager é exibido.

## Acessando o console de manutenção usando o console vSphere VM

Se a interface de usuário do Unified Manager não estiver em operação ou se precisar executar funções que não estejam disponíveis na interface do usuário, você poderá acessar o console de manutenção para reconfigurar seu dispositivo virtual.

### Antes de começar

- Você deve ser o usuário de manutenção.
- O dispositivo virtual deve ser ligado para acessar o console de manutenção.

### Passos

1. No vSphere Client, localize o dispositivo virtual do Unified Manager.
2. Clique na guia **Console**.
3. Clique dentro da janela do console para fazer login.
4. Faça login no console de manutenção usando seu nome de usuário e senha.

Após 15 minutos de inatividade, o console de manutenção faz o logout.

## Menus da consola de manutenção

O console de manutenção consiste em diferentes menus que permitem manter e gerenciar recursos especiais e configurações do servidor do Unified Manager.

Dependendo do sistema operacional no qual você instalou o Unified Manager, o console de manutenção consiste nos seguintes menus:

- Atualizar o Unified Manager (somente VMware)
- Configuração de rede (somente VMware)
- Configuração do sistema (somente VMware)
  - a. Suporte/Diagnóstico
  - b. Repor certificado de servidor
  - c. Fornecedor de dados externo
  - d. Restauração de cópia de segurança
  - e. Configuração do intervalo de polling de desempenho
  - f. Desativar a autenticação SAML
  - g. Exibir/alterar portas de aplicativos
  - h. Configuração do registo de depuração
    - i. Controle o acesso à porta MySQL 3306
  - j. Saia

Selecione o número na lista para aceder à opção de menu específica. Por exemplo, para backup e restauração, selecione 4.

### Menu Network Configuration (Configuração da rede)

O menu Network Configuration (Configuração de rede) permite gerir as definições de rede. Você deve usar esse menu quando a interface de usuário do Unified Manager não estiver disponível.



Esse menu não estará disponível se o Unified Manager estiver instalado no Red Hat Enterprise Linux ou no Microsoft Windows.

Estão disponíveis as seguintes opções de menu.

- **Display IP Address Settings** (Exibir configurações de endereço IP)

Exibe as configurações de rede atuais do dispositivo virtual, incluindo o endereço IP, rede, endereço de broadcast, máscara de rede, gateway e servidores DNS.

- **Altere as configurações de endereço IP**

Permite alterar qualquer uma das definições de rede para o dispositivo virtual, incluindo o endereço IP, máscara de rede, gateway ou servidores DNS. Se você mudar as configurações de rede de DHCP para redes estáticas usando o console de manutenção, não será possível editar o nome do host. Você deve selecionar **Commit Changes** para que as alterações ocorram.

- **Exibir configurações de pesquisa de nome de domínio**

Exibe a lista de pesquisa de nome de domínio usada para resolver nomes de host.

- \* Alterar configurações de pesquisa de nome de domínio\*

Permite alterar os nomes de domínio para os quais você deseja pesquisar ao resolver nomes de host. Você deve selecionar **Commit Changes** para que as alterações ocorram.

- **Exibir rotas estáticas**

Apresenta as rotas de rede estáticas atuais.

- **Alterar rotas estáticas**

Permite adicionar ou eliminar rotas de rede estáticas. Você deve selecionar **Commit Changes** para que as alterações ocorram.

- **Adicionar rota**

Permite adicionar uma rota estática.

- **Eliminar rota**

Permite eliminar uma rota estática.

- \* Voltar\*

Leva-o de volta ao **Menu Principal**.

- **Saída**

Sai da consola de manutenção.

- \* Desativar a interface de rede\*

Desativa todas as interfaces de rede disponíveis. Se apenas uma interface de rede estiver disponível, não é possível desativá-la. Você deve selecionar **Commit Changes** para que as alterações ocorram.

- **Ativar interface de rede**

Permite interfaces de rede disponíveis. Você deve selecionar **Commit Changes** para que as alterações ocorram.

- **Commit Changes**

Aplica quaisquer alterações efetuadas às definições de rede para o dispositivo virtual. Você deve selecionar essa opção para realizar quaisquer alterações feitas ou as alterações não ocorrem.

- **Ping um anfitrião**

Faz pings em um host de destino para confirmar alterações de endereço IP ou configurações de DNS.

- **Restaurar para as configurações padrão**

Repõe todas as definições para as predefinições de fábrica. Você deve selecionar **Commit Changes** para

que as alterações ocorram.

- \* Voltar\*

Leva-o de volta ao **Menu Principal**.

- **Saída**

Sai da consola de manutenção.

## Menu System Configuration (Configuração do sistema)

O menu System Configuration (Configuração do sistema) permite-lhe gerir o seu dispositivo virtual, fornecendo várias opções, tais como a visualização do estado do servidor e a reinicialização e encerramento da máquina virtual.



Quando o Unified Manager é instalado em um sistema Linux ou Microsoft Windows, somente a opção ""Restaurar a partir de um backup do Unified Manager"" está disponível neste menu.

Estão disponíveis as seguintes opções de menu:

- **Estado do servidor de visualização**

Exibe o status atual do servidor. As opções de status incluem Running (Corrida) e Not Running (não corrida).

Se o servidor não estiver em execução, talvez seja necessário entrar em Contato com o suporte técnico.

- **Reboot Virtual Machine**

Reinicializa a máquina virtual, interrompendo todos os serviços. Após a reinicialização, a máquina virtual e os serviços reiniciam.

- **Desligue a máquina virtual**

Desliga a máquina virtual, parando todos os serviços.

Você pode selecionar essa opção somente no console da máquina virtual.

- \* Alterar senha de usuário \*

Altera a palavra-passe do utilizador que está atualmente ligado, que só pode ser o utilizador de manutenção.

- **Aumente o tamanho do disco de dados**

Aumenta o tamanho do disco de dados (disco 3) na máquina virtual.

- **Aumente o tamanho do disco de troca**

Aumenta o tamanho do disco de troca (disco 2) na máquina virtual.

- **Alterar fuso horário**

Altera o fuso horário para a sua localização.

- **Altere o servidor NTP**

Altera as configurações do servidor NTP, como endereço IP ou nome de domínio totalmente qualificado (FQDN).

- **Altere o serviço NTP**

Alterna entre `ntp` os serviços e `systemd-timesyncd`

- **Restaurar a partir de um backup do Unified Manager**

Restaura o banco de dados do Unified Manager e as configurações de uma versão com backup anterior.

- **Redefinir certificado de servidor**

Redefine o certificado de segurança do servidor.

- **Altere o nome de host**

Altera o nome do host no qual o dispositivo virtual está instalado.

- \* Voltar\*

Sai do menu System Configuration (Configuração do sistema) e regressa ao menu Main (Menu principal).

- **Saída**

Sai do menu da consola de manutenção.

## Menu suporte e Diagnóstico

O menu suporte e Diagnóstico permite gerar um pacote de suporte que pode ser enviado ao suporte técnico para assistência na solução de problemas.

Estão disponíveis as seguintes opções de menu:

- **Gerar Pacote de suporte leve**

Permite produzir um pacote de suporte leve que contém apenas 30 dias de Registros e Registros de banco de dados de configuração — exclui dados de desempenho, arquivos de gravação de aquisição e despejo de heap do servidor.

- **Gerar Pacote de suporte**

Permite criar um pacote de suporte completo (arquivo 7-Zip) contendo informações de diagnóstico no diretório inicial do usuário de diagnóstico. Se o seu sistema estiver ligado à Internet, também pode carregar o pacote de suporte para o NetApp.

O arquivo inclui informações geradas por uma mensagem do AutoSupport, o conteúdo do banco de dados do Gerenciador Unificado, dados detalhados sobre os componentes internos do servidor do Gerenciador Unificado e logs de nível detalhado não incluídos normalmente nas mensagens do AutoSupport ou no pacote de suporte leve.

## Opções de menu adicionais

As opções de menu a seguir permitem executar várias tarefas administrativas no servidor do Unified Manager.

Estão disponíveis as seguintes opções de menu:

- **Redefinir certificado de servidor**

Regenera o certificado do servidor HTTPS.

Você pode regenerar o certificado do servidor na GUI do Unified Manager clicando em **Geral > certificados HTTPS > Regenerate HTTPS Certificate**.

- **\* Desativar autenticação SAML\***

Desativa a autenticação SAML para que o provedor de identidade (IDP) não forneça mais autenticação de logon para usuários que acessam a GUI do Unified Manager. Essa opção de console geralmente é usada quando um problema com o servidor IDP ou a configuração SAML impede que os usuários acessem a GUI do Unified Manager.

- **Fornecedor de dados Externo**

Fornece opções para conectar o Unified Manager a um provedor de dados externo. Depois de estabelecer a conexão, os dados de desempenho são enviados para um servidor externo para que os especialistas em desempenho de storage possam traçar as métricas de desempenho usando software de terceiros. São apresentadas as seguintes opções:

- **Configuração do servidor de exibição**--exibe as configurações atuais de conexão e configuração para um provedor de dados externo.
- **Adicionar / Modificar conexão do servidor**--permite que você insira novas configurações de conexão para um provedor de dados externo ou altere as configurações existentes.
- **Modificar configuração do servidor**--permite que você insira novas configurações para um provedor de dados externo ou altere as configurações existentes.
- **Excluir conexão do servidor**--exclui a conexão com um provedor de dados externo.

Depois que a conexão é excluída, o Unified Manager perde sua conexão com o servidor externo.

- **Backup Restore**

Para obter informações, consulte os tópicos em "[Gerenciamento de operações de backup e restauração](#)".

- **Configuração do intervalo de polling de desempenho**

Fornece uma opção para configurar com que frequência o Unified Manager coleta dados estatísticos de desempenho dos clusters. O intervalo de coleta padrão é de 5 minutos.

Você pode alterar esse intervalo para 10 ou 15 minutos se descobrir que coleções de clusters grandes não estão sendo concluídas no tempo.

- **Exibir/alterar portas de aplicativos**

Fornece uma opção para alterar as portas padrão que o Unified Manager usa para protocolos HTTP e HTTPS, se necessário para segurança. As portas padrão são 80 para HTTP e 443 para HTTPS.

- \* Controle o acesso à porta MySQL 3306\*

Controla o acesso do host à porta MySQL padrão 3306. Por razões de segurança, o acesso por meio dessa porta é restrito apenas ao localhost durante uma nova instalação do Unified Manager em sistemas Linux, Windows e VMware vSphere. Essa opção permite alternar a visibilidade dessa porta entre o localhost e os hosts remotos, ou seja, se ela estiver habilitada para localhost somente em seu ambiente, você também poderá disponibilizar essa porta para hosts remotos. Como alternativa, quando ativado para todos os hosts, você pode restringir o acesso desta porta apenas ao localhost. Se o acesso foi ativado em hosts remotos anteriormente, a configuração é mantida em um cenário de atualização. Você deve verificar as configurações de firewall em sistemas Windows depois de alternar a visibilidade da porta e desativar as configurações de firewall se as configurações estiverem configuradas para restringir o acesso à porta MySQL 3306.

- **Saída**

Sai do menu da consola de manutenção.

## Alterar a palavra-passe do utilizador de manutenção no Windows

Você pode alterar a senha do usuário de manutenção do Unified Manager quando necessário.

### Passos

1. Na página de login da IU da Web do Unified Manager, clique em **Esqueceu a senha**.

É apresentada uma página que solicita o nome do utilizador cuja palavra-passe pretende repor.

2. Digite o nome de usuário e clique em **Enviar**.

Um e-mail com um link para redefinir a senha é enviado para o endereço de e-mail definido para esse nome de usuário.

3. Clique no link **RESET password** no e-mail e defina a nova senha.
4. Retorne à IU da Web e faça login no Unified Manager usando a nova senha.

## Alterar a senha umadmin em sistemas Linux

Por motivos de segurança, você deve alterar a senha padrão do usuário umadmin do Unified Manager imediatamente após concluir o processo de instalação. Se necessário, você pode alterar a senha novamente a qualquer momento mais tarde.

### Antes de começar

- O Unified Manager deve ser instalado em um sistema Red Hat Enterprise Linux Linux.
- Você deve ter as credenciais de usuário raiz para o sistema Linux no qual o Unified Manager está instalado.

### Passos

1. Faça login como usuário raiz no sistema Linux no qual o Unified Manager está sendo executado.
2. Altere a senha umadmin:

```
passwd umadmin
```



O sistema solicita que você insira uma nova senha para o usuário umadmin.

## Alterar as portas que o Unified Manager usa para protocolos HTTP e HTTPS

As portas padrão que o Unified Manager usa para protocolos HTTP e HTTPS podem ser alteradas após a instalação, se necessário para segurança. As portas padrão são 80 para HTTP e 443 para HTTPS.

### Antes de começar

Você deve ter uma ID de usuário e senha autorizados para fazer login no console de manutenção do servidor do Unified Manager.



Existem algumas portas que são consideradas inseguras ao usar os navegadores Mozilla Firefox ou Google Chrome. Verifique com o navegador antes de atribuir um novo número de porta para o tráfego HTTP e HTTPS. Selecionar uma porta insegura pode tornar o sistema inacessível, o que exigiria que você entre em Contato com o suporte ao cliente para obter uma resolução.

A instância do Unified Manager é reiniciada automaticamente depois de alterar a porta, portanto, certifique-se de que este é um bom momento para desativar o sistema por um curto período de tempo.

1. Faça login usando SSH como o usuário de manutenção no host do Unified Manager.

Os prompts do console do Unified Managermaintenance são exibidos.

2. Digite o número da opção de menu chamada **Exibir/alterar portas do aplicativo** e pressione Enter.
3. Se solicitado, digite a senha do usuário de manutenção novamente.
4. Digite os novos números de porta para as portas HTTP e HTTPS e pressione Enter.

Deixar um número de porta em branco atribui a porta padrão para o protocolo.

Você será solicitado a alterar as portas e reiniciar o Unified Manager agora.

5. Digite **y** para alterar as portas e reiniciar o Unified Manager.
6. Saia da consola de manutenção.

Após essa alteração, os usuários devem incluir o novo número de porta no URL para acessar a interface da Web do Gerenciador Unificado, por exemplo, <https://host.company.com:1234+>, <https://12.13.14.15:1122+>, ou [https://\[2001:db8:0:1\]:2123+](https://[2001:db8:0:1]:2123+).

## Adicionando interfaces de rede

Você pode adicionar novas interfaces de rede se precisar separar o tráfego de rede.

### Antes de começar

Você deve ter adicionado a interface de rede ao dispositivo virtual usando o vSphere.

O dispositivo virtual deve estar ligado.



Não é possível executar esta operação se o Unified Manager estiver instalado no Red Hat Enterprise Linux ou no Microsoft Windows.

## Passos

1. No menu principal do console vSphere, selecione **Configuração do sistema > Reboot Operating System**.

Após a reinicialização, o console de manutenção pode detetar a interface de rede recém-adicionada.

2. Aceda à consola de manutenção.
3. Selecione **Configuração de rede > Ativar Interface de rede**.
4. Selecione a nova interface de rede e pressione **Enter**.

Selecione **eth1** e pressione **Enter**.

5. Digite **y** para ativar a interface de rede.
6. Introduza as definições de rede.

É-lhe pedido que introduza as definições de rede se estiver a utilizar uma interface estática ou se o DHCP não for detetado.

Depois de introduzir as definições de rede, regressa automaticamente ao menu **Configuração de rede**.

7. Selecione **Commit Changes**.

Você deve confirmar as alterações para adicionar a interface de rede.

## Adicionando espaço em disco ao diretório do banco de dados do Unified Manager

O diretório do banco de dados do Unified Manager contém todos os dados de integridade e desempenho coletados dos sistemas ONTAP. Algumas circunstâncias podem exigir que você aumente o tamanho do diretório do banco de dados.

Por exemplo, o diretório do banco de dados pode ficar cheio se o Unified Manager estiver coletando dados de um grande número de clusters onde cada cluster tem muitos nós. Você receberá um evento de aviso quando o diretório do banco de dados estiver 90% cheio e um evento crítico quando o diretório estiver 95% cheio.



Nenhum dado adicional é coletado de clusters depois que o diretório atinge 95% cheio.

As etapas necessárias para adicionar capacidade ao diretório de dados são diferentes dependendo se o Unified Manager está sendo executado em um servidor VMware ESXi, em um servidor Red Hat ou em um servidor Microsoft Windows.

### Adicionando espaço ao diretório de dados do host Linux

Se você atribuiu espaço em disco insuficiente ao `/opt/netapp/data` diretório para oferecer suporte ao Unified Manager quando configurou originalmente o host Linux e instalou o Unified Manager, você poderá adicionar espaço em disco após a instalação aumentando o espaço em disco `/opt/netapp/data` no diretório.

## Antes de começar

Você deve ter acesso de usuário raiz à máquina Red Hat Enterprise Linux na qual o Unified Manager está instalado.

Recomendamos que você faça backup do banco de dados do Unified Manager antes de aumentar o tamanho do diretório de dados.

## Passos

1. Faça login como usuário root na máquina Linux na qual você deseja adicionar espaço em disco.
2. Pare o serviço Unified Manager e o software MySQL associado na ordem mostrada:

```
systemctl stop ocieau ocie mysqld
```

3. Crie uma pasta de backup temporária (por exemplo, /backup-data) com espaço em disco suficiente para conter os dados no diretório atual /opt/netapp/data.
4. Copie o conteúdo e a configuração de privilégios do diretório existente /opt/netapp/data para o diretório de dados de backup:

```
cp -arp /opt/netapp/data/* /backup-data
```

5. Se o se Linux estiver ativado:

- a. Obtenha o tipo se Linux para pastas na pasta existente /opt/netapp/data:

```
se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1
```

O sistema retorna uma confirmação semelhante à seguinte:

```
echo $se_type  
mysqld_db_t
```

- a. Execute o comando chcon para definir o tipo se Linux para o diretório de backup:

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Remova o conteúdo do /opt/netapp/data diretório:

- a. `cd /opt/netapp/data`

- b. `rm -rf *`

7. Expanda o tamanho /opt/netapp/data do diretório para um mínimo de 150 GB por meio de comandos LVM ou adicionando discos extras.



Se você criou /opt/netapp/data a partir de um disco, então você não deve tentar montar /opt/netapp/data como um compartilhamento NFS ou CIFS. Porque, neste caso, se você tentar expandir o espaço em disco, alguns comandos LVM, `resize` como e `extend` podem não funcionar como esperado.

8. Confirme que o /opt/netapp/data proprietário do diretório (mysql) e o grupo (root) estão inalterados:

```
ls -ltr /opt/netapp/ | grep data
```

O sistema retorna uma confirmação semelhante à seguinte:

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. Se o se Linux estiver ativado, confirme que o contexto `/opt/netapp/data` do diretório ainda está definido como `mysqld_db_t`:

a. `touch /opt/netapp/data/abc`

b. `ls -Z /opt/netapp/data/abc`

O sistema retorna uma confirmação semelhante à seguinte:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0  
/opt/netapp/data/abc
```

10. Exclua o arquivo `abc` para que esse arquivo estranho não cause um erro de banco de dados no futuro.

11. Copie o conteúdo dos dados de backup de volta para o diretório expandido `/opt/netapp/data`:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Se o se Linux estiver ativado, execute o seguinte comando:

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. Inicie o serviço MySQL:

```
systemctl start mysqld
```

14. Após o início do serviço MySQL, inicie os serviços `ocie` e `ocieau` na ordem mostrada:

```
systemctl start ocie ocieau
```

15. Depois de todos os serviços serem iniciados, exclua a pasta de `/backup-data` `backup` :

```
rm -rf /backup-data
```

## Adicionando espaço ao disco de dados da máquina virtual VMware

Se você precisar aumentar a quantidade de espaço no disco de dados para o banco de dados do Unified Manager, poderá adicionar capacidade após a instalação aumentando o espaço em disco usando o console de manutenção do Unified Manager.

### Antes de começar

- Você deve ter acesso ao vSphere Client.
- A máquina virtual não deve ter instantâneos armazenados localmente.

- Tem de ter as credenciais do utilizador de manutenção.

Recomendamos que você faça backup de sua máquina virtual antes de aumentar o tamanho dos discos virtuais.

### Passos

1. No cliente vSphere, selecione a máquina virtual do Unified Manager e adicione mais capacidade de disco aos dados `disk 3`. Consulte a documentação da VMware para obter detalhes.

Em alguns casos raros, a implantação do Unified Manager usa o disco rígido 2 para o disco de dados em vez do disco rígido 3. Se isso tiver ocorrido em sua implantação, aumente o espaço de qualquer disco maior. O disco de dados sempre terá mais espaço do que o outro disco.

2. No cliente vSphere, selecione a máquina virtual do Unified Manager e, em seguida, selecione a guia **Console**.
3. Clique na janela do console e, em seguida, faça login no console de manutenção usando seu nome de usuário e senha.
4. No Menu Principal, introduza o número para a opção **Configuração do sistema**.
5. No menu Configuração do sistema, insira o número da opção **aumentar o tamanho do disco de dados**.

### Adicionando espaço à unidade lógica do servidor Microsoft Windows

Se você precisar aumentar a quantidade de espaço em disco para o banco de dados do Unified Manager, poderá adicionar capacidade à unidade lógica na qual o Unified Manager está instalado.

#### Antes de começar

Você deve ter o Privilegio administrador do Windows.

Recomendamos que você faça backup do banco de dados do Unified Manager antes de adicionar espaço em disco.

### Passos

1. Inicie sessão como administrador no servidor Windows no qual pretende adicionar espaço em disco.
2. Siga a etapa que corresponde ao método que você deseja usar para adicionar mais espaço:

Opção	Descrição
Em um servidor físico, adicione capacidade à unidade lógica na qual o servidor do Unified Manager está instalado.	Siga as etapas no tópico da Microsoft: <a href="#">"Estender um volume básico"</a>
Em um servidor físico, adicione uma unidade de disco rígido.	Siga as etapas no tópico da Microsoft: <a href="#">"Adicionar unidades de disco rígido"</a>
Em uma máquina virtual, aumente o tamanho de uma partição de disco.	Siga as etapas no tópico VMware: <a href="#">"Aumentando o tamanho de uma partição de disco"</a>

# Gerenciando o acesso do usuário

Você pode criar funções e atribuir recursos para controlar o acesso do usuário ao Active IQ Unified Manager. Você pode identificar usuários que têm os recursos necessários para acessar objetos selecionados no Unified Manager. Somente os usuários que têm essas funções e recursos podem gerenciar os objetos no Unified Manager.

## Adicionando usuários

Você pode adicionar usuários locais ou usuários de banco de dados usando a página usuários. Você também pode adicionar usuários remotos ou grupos que pertencem a um servidor de autenticação. Você pode atribuir funções a esses usuários e, com base no Privileges das funções, os usuários podem gerenciar os objetos de storage e dados com o Unified Manager, ou exibir os dados em um banco de dados.

### Antes de começar

- Tem de ter a função Administrador de aplicações.
- Para adicionar um utilizador ou grupo remoto, tem de ter ativado a autenticação remota e configurado o servidor de autenticação.
- Se você planeja configurar a autenticação SAML para que um provedor de identidade (IDP) autentique usuários acessando a interface gráfica, certifique-se de que esses usuários sejam definidos como usuários "remode".

O acesso à IU não é permitido para usuários do tipo "local" ou "Manutenção" quando a autenticação SAML está ativada.

Se você adicionar um grupo do Windows active Directory, todos os membros diretos e subgrupos aninhados poderão se autenticar no Unified Manager, a menos que os subgrupos aninhados estejam desativados. Se você adicionar um grupo do OpenLDAP ou de outros serviços de autenticação, somente os membros diretos desse grupo poderão se autenticar no Unified Manager.

### Passos

1. No painel de navegação esquerdo, clique em **Geral > usuários**.
2. Na página usuários, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar usuário, selecione o tipo de usuário que deseja adicionar e insira as informações necessárias.

Ao inserir as informações de usuário necessárias, você deve especificar um endereço de e-mail exclusivo para esse usuário. Você deve evitar especificar endereços de e-mail compartilhados por vários usuários.

4. Clique em **Add**.

### Criando um usuário de banco de dados

Para oferecer suporte a uma conexão entre o Workflow Automation e o Unified Manager, ou para acessar exibições de banco de dados, primeiro é necessário criar um usuário de banco de dados com a função Esquema de integração ou Esquema de Relatório na IU da Web do Unified Manager.

## Antes de começar

Tem de ter a função Administrador de aplicações.

Os usuários de banco de dados fornecem integração com o Workflow Automation e acesso a visualizações de banco de dados específicas de relatórios. Os usuários de banco de dados não têm acesso à IU da Web do Unified Manager nem ao console de manutenção e não podem executar chamadas de API.

## Passos

1. No painel de navegação esquerdo, clique em **Geral > usuários**.
2. Na página usuários, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar usuário, selecione **Usuário de banco de dados** na lista suspensa **tipo**.
4. Digite um nome e uma senha para o usuário do banco de dados.
5. Na lista suspensa **Role**, selecione a função apropriada.

Se você é...	Escolha esta função
Conetando o Unified Manager ao Workflow Automation	Esquema de integração
Acessando relatórios e outras exibições de banco de dados	Esquema Relatório

6. Clique em **Add**.

## Editar as definições do utilizador

Você pode editar as configurações do usuário - como o endereço de e-mail e a função - que são especificadas cada usuário. Por exemplo, talvez você queira alterar a função de um usuário que é um operador de armazenamento e atribuir Privileges ao usuário do administrador de armazenamento.

## Antes de começar

Tem de ter a função Administrador de aplicações.

Quando você modifica a função atribuída a um usuário, as alterações são aplicadas quando uma das seguintes ações ocorre:

- O usuário faz logout e faz login novamente no Unified Manager.
- O tempo limite da sessão de 24 horas é atingido.

## Passos

1. No painel de navegação esquerdo, clique em **Geral > usuários**.
2. Na página usuários, selecione o usuário para o qual deseja editar as configurações e clique em **Editar**.
3. Na caixa de diálogo Editar usuário, edite as configurações apropriadas especificadas para o usuário.
4. Clique em **Salvar**.

## Visualização de usuários

Você pode usar a página usuários para exibir a lista de usuários que gerenciam dados e objetos de storage usando o Unified Manager. Você pode exibir detalhes sobre os usuários, como nome de usuário, tipo de usuário, endereço de e-mail e a função atribuída aos usuários.

### Antes de começar

Tem de ter a função Administrador de aplicações.

### Passo

1. No painel de navegação esquerdo, clique em **Geral > usuários**.

## Eliminar utilizadores ou grupos

É possível excluir um ou mais usuários do banco de dados do servidor de gerenciamento para impedir que usuários específicos acessem o Unified Manager. Você também pode excluir grupos para que todos os usuários do grupo não possam mais acessar o servidor de gerenciamento.

### Antes de começar

- Ao excluir grupos remotos, você deve ter reatribuído os eventos atribuídos aos usuários dos grupos remotos.

Se você estiver excluindo usuários locais ou usuários remotos, os eventos atribuídos a esses usuários serão automaticamente não atribuídos.

- Tem de ter a função Administrador de aplicações.

### Passos

1. No painel de navegação esquerdo, clique em **Geral > usuários**.
2. Na página usuários, selecione os usuários ou grupos que você deseja excluir e clique em **Excluir**.
3. Clique em **Yes** para confirmar a exclusão.

## O que é RBAC

O RBAC (controle de acesso baseado em função) permite controlar quem tem acesso a vários recursos e recursos no servidor Active IQ Unified Manager.

## Que controle de acesso baseado em função faz

O controle de acesso baseado em função (RBAC) permite que os administradores gerenciem grupos de usuários definindo funções. Se você precisar restringir o acesso para funcionalidades específicas aos administradores selecionados, você deverá configurar contas de administrador para eles. Se você quiser restringir as informações que os administradores podem exibir e as operações que podem executar, você deve aplicar funções às contas de administrador criadas.



O servidor de gerenciamento usa o RBAC para login de usuário e permissões de função. Se você não alterou as configurações padrão do servidor de gerenciamento para acesso administrativo ao usuário, não será necessário fazer login para visualizá-las.

Quando você inicia uma operação que requer Privileges específico, o servidor de gerenciamento solicita que você faça login. Por exemplo, para criar contas de administrador, você deve fazer login com acesso à conta de Administrador de aplicativos.

## Definições dos tipos de utilizador

Um tipo de usuário especifica o tipo de conta que o usuário detém e inclui usuários remotos, grupos remotos, usuários locais, usuários de banco de dados e usuários de manutenção. Cada um desses tipos tem sua própria função, que é atribuída por um usuário com a função de Administrador.

Os tipos de usuário do Unified Manager são os seguintes:

- **Usuário de manutenção**

Criado durante a configuração inicial do Unified Manager. O usuário de manutenção cria usuários adicionais e atribui funções. O utilizador de manutenção é também o único utilizador com acesso à consola de manutenção. Quando o Unified Manager é instalado em um sistema Red Hat Enterprise Linux, o usuário de manutenção recebe o nome de usuário "umadmin".

- **Usuário local**

Acessa a IU do Unified Manager e executa funções com base na função dada pelo usuário de manutenção ou por um usuário com a função Administrador de aplicativos.

- **Grupo remoto**

Um grupo de usuários que acessam a IU do Unified Manager usando as credenciais armazenadas no servidor de autenticação. O nome desta conta deve corresponder ao nome de um grupo armazenado no servidor de autenticação. Todos os usuários do grupo remoto têm acesso à IU do Unified Manager usando suas credenciais de usuário individuais. Os grupos remotos podem executar funções de acordo com suas funções atribuídas.

- **Utilizador remoto**

Acessa a IU do Unified Manager usando as credenciais armazenadas no servidor de autenticação. Um usuário remoto executa funções com base na função dada pelo usuário de manutenção ou um usuário com a função Administrador de aplicativos.

- **Usuário do banco de dados**

Tem acesso somente leitura aos dados no banco de dados do Unified Manager, não tem acesso à interface da Web do Unified Manager nem ao console de manutenção e não pode executar chamadas de API.

## Definições de funções de utilizador

O usuário de manutenção ou o administrador de aplicativos atribui uma função a cada usuário. Cada função contém determinados Privileges. O escopo das atividades que

o que voc3e pode executar no Unified Manager depende da fun77o atribu3da e de qual Privileges a fun77o cont3m.

O Unified Manager inclui as seguintes fun77es de usu3rio predefinidas:

- **Operador**

Exibe informa77es do sistema de storage e outros dados coletados pelo Unified Manager, incluindo hist3ricos e tend3ncias de capacidade. Essa fun77o permite que o operador de armazenamento exiba, atribua, reconhe77a, resolva e adicione notas para os eventos.

- **Administrador de armazenamento**

Configura as opera77es de gerenciamento de storage no Unified Manager. Essa fun77o permite que o administrador de storage configure limites e crie alertas e outras op77es e pol3ticas espec3ficas de gerenciamento de storage.

- **Administrador de aplica77o**

Configura configura77es n3o relacionadas ao gerenciamento de armazenamento. Essa fun77o permite o gerenciamento de usu3rios, certificados de seguran77a, acesso a banco de dados e op77es administrativas, incluindo autentica77o, SMTP, rede e AutoSupport.



Quando o Unified Manager 3 instalado em sistemas Linux, o usu3rio inicial com a fun77o Application Administrator 3 automaticamente chamado de "umadmin".

- **Esquema de integra77o**

Essa fun77o permite o acesso somente leitura 3s visualiza77es do banco de dados do Unified Manager para integrar o Unified Manager ao OnCommand Workflow Automation (WFA).

- **Esquema Relat3rio**

Essa fun77o permite o acesso somente leitura a relat3rios e outras visualiza77es de banco de dados diretamente do banco de dados do Unified Manager. Os bancos de dados que podem ser visualizados incluem:

- NetApp\_model\_view
- NetApp\_performance
- ocum
- ocum\_report
- ocum\_report\_birt
- opm
- scalemonitor

## Fun77es e recursos de usu3rio do Unified Manager

Com base na fun77o de usu3rio atribu3da, voc3e pode determinar quais opera77es podem ser executadas no Unified Manager.

A tabela a seguir exibe as fun77es que cada fun77o de usu3rio pode executar:

<b>Função</b>	<b>Operador</b>	<b>Administrador de armazenamento</b>	<b>Administrador de aplicativos</b>	<b>Esquema de integração</b>	<b>Esquema Relatório</b>
Ver informações do sistema de armazenamento	•	•	•	•	•
Veja outros dados, como históricos e tendências de capacidade	•	•	•	•	•
Exibir, atribuir e resolver eventos	•	•	•		
Visualize objetos do serviço de storage, como associações de SVM e pools de recursos	•	•	•		
Exibir políticas de limite	•	•	•		
Gerenciar objetos de serviço de storage, como associações de SVM e pools de recursos		•	•		
Definir alertas		•	•		
Gerenciar opções de gerenciamento de storage		•	•		
Gerenciar políticas de gerenciamento de storage		•	•		
Gerenciar usuários			•		

Função	Operador	Administrador de armazenamento	Administrador de aplicativos	Esquema de integração	Esquema Relatório
Gerenciar opções administrativas			•		
Definir políticas de limite			•		
Gerenciar acesso ao banco de dados			•		
Gerencie a integração com O WFA e forneça acesso às visualizações do banco de dados				•	
Programe e salve relatórios		•	•		
Execute as operações "Fix it" a partir de ações de gerenciamento		•	•		
Forneça acesso somente leitura às exibições do banco de dados					•

## Gerenciando configurações de autenticação SAML

Depois de configurar as configurações de autenticação remota, é possível ativar a autenticação SAML (Security Assertion Markup Language) para que os usuários remotos sejam autenticados por um provedor de identidade seguro (IDP) antes que eles possam acessar a IU da Web do Unified Manager.

Observe que somente usuários remotos terão acesso à interface gráfica do usuário do Unified Manager depois que a autenticação SAML for ativada. Os utilizadores locais e os utilizadores de manutenção não poderão aceder à IU. Essa configuração não afeta os usuários que acessam o console de manutenção.

## Requisitos do provedor de identidade

Ao configurar o Unified Manager para usar um provedor de identidade (IDP) para executar a autenticação SAML para todos os usuários remotos, você precisa estar ciente de algumas configurações necessárias para que a conexão com o Unified Manager seja bem-sucedida.

É necessário inserir o URI e os metadados do Unified Manager no servidor IDP. Você pode copiar essas informações da página Autenticação do Unified Manager SAML. O Unified Manager é considerado o provedor de serviços (SP) no padrão SAML (Security Assertion Markup Language).

### Padrões de criptografia suportados

- AES (Advanced Encryption Standard): AES-128 e AES-256
- Algoritmo Hash seguro (SHA): SHA-1 e SHA-256

### Provedores de identidade validados

- Shibboleth
- Serviços de Federação do Active Directory (ADFS)

### Requisitos de configuração ADFS

- Você deve definir três regras de reivindicação na ordem a seguir, necessárias para que o Unified Manager analise respostas ADFS SAML para essa entrada confiável de parte confiável.

Regra de reclamação	Valor
Nome da conta SAM	ID do nome
Nome da conta SAM	urna:oid:0.9.2342.19200300.100.1.1
Grupos de token — Nome não qualificado	urna:oid:1.3.6.1.4.1.5923.1.5.1.1

- Você deve definir o método de autenticação como ""Autenticação de formulários"" ou os usuários podem receber um erro ao fazer logout do Unified Manager . Siga estes passos:
  - a. Abra o Console de Gerenciamento ADFS.
  - b. Clique na pasta Authentication Policies (políticas de autenticação) no modo de exibição de árvore à esquerda.
  - c. Em ações à direita, clique em Editar política de autenticação primária global.
  - d. Defina o método de autenticação da Intranet como ""Autenticação de formulários"" em vez da "Autenticação do Windows" padrão.
- Em alguns casos, o login pelo IDP é rejeitado quando o certificado de segurança do Unified Manager é assinado pela CA. Existem duas soluções alternativas para resolver este problema:
  - Siga as instruções identificadas no link para desativar a verificação de revogação no servidor ADFS para a entidade dependente associada a cert AC encadeada:

["Desativar Verificação de revogação por confiança de parte dependente"](#)

- Peça que o servidor da CA resida no servidor ADFS para assinar a solicitação de cert do servidor do Unified Manager.

## Outros requisitos de configuração

- O desvio do relógio do Unified Manager é definido para 5 minutos, portanto, a diferença de tempo entre o servidor IDP e o servidor do Unified Manager não pode ser superior a 5 minutos ou a autenticação falhará.

## Habilitando a autenticação SAML

Você pode ativar a autenticação SAML (Security Assertion Markup Language) para que os usuários remotos sejam autenticados por um provedor de identidade seguro (IDP) antes que eles possam acessar a IU da Web do Unified Manager.

### Antes de começar

- Você deve ter configurado a autenticação remota e verificado se ela foi bem-sucedida.
- Você deve ter criado pelo menos um Usuário remoto ou um Grupo remoto com a função Administrador do aplicativo.
- O provedor de identidade (IDP) deve ser suportado pelo Unified Manager e deve ser configurado.
- Você deve ter o URL e os metadados do IDP.
- Você deve ter acesso ao servidor IDP.

Depois de ativar a autenticação SAML do Unified Manager, os usuários não poderão acessar a interface gráfica do usuário até que o IDP tenha sido configurado com as informações do host do servidor Unified Manager. Portanto, você deve estar preparado para concluir ambas as partes da conexão antes de iniciar o processo de configuração. O IDP pode ser configurado antes ou depois da configuração do Unified Manager.

Somente usuários remotos terão acesso à interface gráfica do usuário do Unified Manager após a autenticação SAML ser ativada. Os utilizadores locais e os utilizadores de manutenção não poderão aceder à IU. Essa configuração não afeta os usuários que acessam o console de manutenção, os comandos do Unified Manager ou ZAPIs.



O Unified Manager é reiniciado automaticamente após concluir a configuração SAML nesta página.

### Passos

1. No painel de navegação à esquerda, clique em **Geral > Autenticação SAML**.
2. Marque a caixa de seleção **Enable SAML Authentication** (Ativar autenticação SAML\*).

São apresentados os campos necessários para configurar a ligação IDP.

3. Insira o URI de IDP e os metadados de IDP necessários para conectar o servidor do Unified Manager ao servidor de IDP.

Se o servidor IDP estiver acessível diretamente a partir do servidor do Unified Manager, você poderá clicar no botão **obter metadados IDP** depois de inserir o URI IDP para preencher o campo metadados IDP automaticamente.

4. Copie o URI de metadados do host do Unified Manager ou salve os metadados do host em um arquivo de texto XML.

Neste momento, você pode configurar o servidor IDP com essas informações.

5. Clique em **Salvar**.

Uma caixa de mensagem é exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

6. Clique em **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.

Da próxima vez que os usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do IDP em vez da página de login do Unified Manager.

Se ainda não estiver concluído, acesse seu IDP e insira o URI e os metadados do servidor do Unified Manager para concluir a configuração.



Ao usar o ADFS como provedor de identidade, a GUI do Unified Manager não honra o tempo limite do ADFS e continuará funcionando até que o tempo limite da sessão do Unified Manager seja atingido. Você pode alterar o tempo limite da sessão da GUI clicando em **Geral > Configurações da função > tempo limite de inatividade**.

## Alterar o provedor de identidade usado para autenticação SAML

Você pode alterar o provedor de identidade (IDP) que o Unified Manager usa para autenticar usuários remotos.

### Antes de começar

- Você deve ter o URL e os metadados do IDP.
- Você deve ter acesso ao IDP.

O novo IDP pode ser configurado antes ou depois da configuração do Unified Manager.

### Passos

1. No painel de navegação à esquerda, clique em **Geral > Autenticação SAML**.
2. Insira o novo URI de IDP e os metadados de IDP necessários para conectar o servidor do Unified Manager ao IDP.

Se o IDP estiver acessível diretamente a partir do servidor do Unified Manager, você poderá clicar no botão **obter metadados IDP** depois de inserir o URL IDP para preencher o campo metadados IDP automaticamente.

3. Copie o URI de metadados do Unified Manager ou salve os metadados em um arquivo de texto XML.
4. Clique em **Save Configuration** (Guardar configuração).

É apresentada uma caixa de mensagem para confirmar que pretende alterar a configuração.

5. Clique em **OK**.

Acesse o novo IDP e insira o URI e os metadados do servidor do Unified Manager para concluir a configuração.

Da próxima vez que os usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na nova página de login do IDP em vez da antiga página de login do IDP.

## Atualizando as configurações de autenticação SAML após a alteração do certificado de segurança do Unified Manager

Qualquer alteração ao certificado de segurança HTTPS instalado no servidor do Unified Manager requer que você atualize as configurações de autenticação SAML. O certificado é atualizado se você renomear o sistema host, atribuir um novo endereço IP para o sistema host ou alterar manualmente o certificado de segurança do sistema.

Depois que o certificado de segurança for alterado e o servidor do Unified Manager for reiniciado, a autenticação SAML não funcionará e os usuários não poderão acessar a interface gráfica do Unified Manager. Você deve atualizar as configurações de autenticação SAML no servidor IDP e no servidor Unified Manager para reativar o acesso à interface do usuário.

### Passos

1. Inicie sessão na consola de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

Uma mensagem é exibida para confirmar que você deseja desativar a autenticação SAML e reiniciar o Unified Manager.

3. Inicie a interface de usuário do Unified Manager usando o FQDN ou o endereço IP atualizado, aceite o certificado de servidor atualizado no navegador e faça login usando as credenciais de usuário de manutenção.
4. Na página **Configuração/Autenticação**, selecione a guia **Autenticação SAML** e configure a conexão IDP.
5. Copie o URI de metadados do host do Unified Manager ou salve os metadados do host em um arquivo de texto XML.
6. Clique em **Salvar**.

Uma caixa de mensagem é exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

7. Clique em **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.
8. Acesse seu servidor IDP e insira o URI e os metadados do servidor Unified Manager para concluir a configuração.

Provedor de identidade	Etapas de configuração
ADFS	<ol style="list-style-type: none"><li>a. Exclua a entrada confiável de parte confiável existente na GUI de gerenciamento ADFS.</li><li>b. Adicione uma nova entrada confiável de parte confiável usando o <code>saml_sp_metadata.xml</code> do servidor Unified Manager atualizado.</li><li>c. Defina as três regras de reivindicação necessárias para que o Unified Manager analise respostas ADFS SAML para essa entrada confiável de parte confiável.</li><li>d. Reinicie o serviço ADFS Windows.</li></ol>



Provedor de identidade	Etapas de configuração
Shibboleth	<ol style="list-style-type: none"> <li>Atualize o novo FQDN do servidor do Unified Manager para <code>attribute-filter.xml</code> os arquivos e <code>relying-party.xml</code></li> <li>Reinicie o servidor web Apache Tomcat e aguarde até que a porta 8005 fique online.</li> </ol>

9. Faça login no Unified Manager e verifique se a autenticação SAML funciona como esperado por meio do IDP.

## Desativando a autenticação SAML

Você pode desativar a autenticação SAML quando quiser parar de autenticar usuários remotos por meio de um provedor de identidade seguro (IDP) antes que eles possam fazer login na IU da Web do Unified Manager. Quando a autenticação SAML está desativada, os provedores de serviços de diretório configurados, como o ativo Directory ou LDAP, executam a autenticação de logon.

Depois de desativar a autenticação SAML, os utilizadores locais e os utilizadores de manutenção poderão aceder à interface gráfica do utilizador, além dos utilizadores remotos configurados.

Você também pode desativar a autenticação SAML usando o console de manutenção do Unified Manager se não tiver acesso à interface gráfica do usuário.



O Unified Manager é reiniciado automaticamente após a autenticação SAML ser desativada.

### Passos

1. No painel de navegação à esquerda, clique em **Geral > Autenticação SAML**.
2. Desmarque a caixa de seleção **Enable SAML Authentication** (Ativar autenticação SAML\*).
3. Clique em **Salvar**.

Uma caixa de mensagem é exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

4. Clique em **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.

Na próxima vez que os usuários remotos tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do Unified Manager em vez da página de login do IDP.

Acesse seu IDP e exclua o URI e os metadados do servidor do Unified Manager.

## Desativar a autenticação SAML a partir do console de manutenção

Talvez seja necessário desativar a autenticação SAML do console de manutenção quando não houver acesso à GUI do Unified Manager. Isso pode acontecer em casos de má configuração ou se o IDP não estiver acessível.

### Antes de começar

Você deve ter acesso ao console de manutenção como usuário de manutenção.

Quando a autenticação SAML está desativada, os provedores de serviços de diretório configurados, como o ativo Directory ou LDAP, executam a autenticação de logon. Usuários locais e usuários de manutenção poderão acessar a interface gráfica do usuário além de usuários remotos configurados.

Você também pode desativar a autenticação SAML na página Configuração/Autenticação na IU.



O Unified Manager é reiniciado automaticamente após a autenticação SAML ser desativada.

### Passos

1. Inicie sessão na consola de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

Uma mensagem é exibida para confirmar que você deseja desativar a autenticação SAML e reiniciar o Unified Manager.

3. Digite **y** e pressione Enter e o Unified Manager será reiniciado.

Na próxima vez que os usuários remotos tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do Unified Manager em vez da página de login do IDP.

Se necessário, acesse seu IDP e exclua o URL e os metadados do servidor do Unified Manager.

## Página Autenticação SAML

Você pode usar a página Autenticação SAML para configurar o Unified Manager para autenticar usuários remotos usando SAML por meio de um provedor de identidade seguro (IDP) antes que eles possam fazer login na IU da Web do Unified Manager.

- Você deve ter a função Administrador do aplicativo para criar ou modificar a configuração SAML.
- Tem de ter configurado a autenticação remota.
- Você deve ter configurado pelo menos um usuário remoto ou grupo remoto.

Depois que a autenticação remota e os usuários remotos tiverem sido configurados, você poderá selecionar a caixa de seleção Habilitar autenticação SAML para habilitar a autenticação usando um provedor de identidade seguro.

- \* IDP URI\*

O URI para acessar o IDP a partir do servidor do Unified Manager. Exemplos de URIs estão listados abaixo.

Exemplo de URI de ADFS:

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml
```

Exemplo de Shibboleth URI:

```
https://centos7.ntap2016.local/idp/shibboleth
```

- **Metadados IDP**

Os metadados IDP em formato XML.

Se o URL de IDP estiver acessível a partir do servidor do Unified Manager, você pode clicar no botão **obter metadados de IDP** para preencher este campo.

- **Sistema anfitrião (FQDN)**

O FQDN do sistema host do Unified Manager, conforme definido durante a instalação. Você pode alterar esse valor, se necessário.

- \* Host URI\*

O URI para acessar o sistema host do Unified Manager a partir do IDP.

- **Metadados do host**

Os metadados do sistema anfitrião em formato XML.

## Gerenciamento da autenticação

Você pode ativar a autenticação usando LDAP ou Active Directory no servidor do Unified Manager e configurá-la para funcionar com seus servidores para autenticar usuários remotos.

Para ativar a autenticação remota, configurar serviços de autenticação e adicionar severs de autenticação, consulte a seção anterior em **Configurando o Unified Manager para enviar notificações de alerta**.

### Editando servidores de autenticação

Você pode alterar a porta que o servidor do Unified Manager usa para se comunicar com o servidor de autenticação.

#### Antes de começar

Tem de ter a função Administrador de aplicações.

#### Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação remota**.
2. Marque a caixa **Desativar pesquisa de grupo aninhado**.
3. Na área **servidores de autenticação**, selecione o servidor de autenticação que deseja editar e clique em **Editar**.
4. Na caixa de diálogo **Editar servidor de autenticação**, edite os detalhes da porta.
5. Clique em **Salvar**.

### Eliminar servidores de autenticação

Você pode excluir um servidor de autenticação se quiser impedir que o servidor do Unified Manager se comunique com o servidor de autenticação. Por exemplo, se

pretender alterar um servidor de autenticação com o qual o servidor de gestão está a comunicar, pode eliminar o servidor de autenticação e adicionar um novo servidor de autenticação.

### Antes de começar

Tem de ter a função Administrador de aplicações.

Quando você exclui um servidor de autenticação, usuários remotos ou grupos do servidor de autenticação não poderão mais acessar o Unified Manager.

### Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação remota**.
2. Selecione um ou mais servidores de autenticação que você deseja excluir e clique em **Excluir**.
3. Clique em **Yes** para confirmar a solicitação de exclusão.

Se a opção **usar conexão segura** estiver ativada, os certificados associados ao servidor de autenticação serão excluídos juntamente com o servidor de autenticação.

## Autenticação com active Directory ou OpenLDAP

Você pode ativar a autenticação remota no servidor de gerenciamento e configurar o servidor de gerenciamento para se comunicar com seus servidores de autenticação para que os usuários dentro dos servidores de autenticação possam acessar o Unified Manager.

Você pode usar um dos seguintes serviços de autenticação predefinidos ou especificar seu próprio serviço de autenticação:

- Microsoft active Directory



Você não pode usar o Microsoft Lightweight Directory Services.

- OpenLDAP

Você pode selecionar o serviço de autenticação necessário e adicionar os servidores de autenticação apropriados para permitir que os usuários remotos no servidor de autenticação acessem o Unified Manager. As credenciais para usuários remotos ou grupos são mantidas pelo servidor de autenticação. O servidor de gerenciamento usa o LDAP (Lightweight Directory Access Protocol) para autenticar usuários remotos no servidor de autenticação configurado.

Para usuários locais criados no Unified Manager, o servidor de gerenciamento mantém seu próprio banco de dados de nomes de usuário e senhas. O servidor de gerenciamento executa a autenticação e não usa o active Directory ou o OpenLDAP para autenticação.

## Registo de auditoria

Você pode detetar se os logs de auditoria foram comprometidos com o uso de logs de auditoria. Todas as atividades realizadas por um utilizador são monitorizadas e registadas nos registos de auditoria. As auditorias são realizadas para todas as interfaces de usuário e funcionalidades do Active IQ Unified Manager das APIs expostas

publicamente.

Você pode usar o **Registro de auditoria: Exibição de arquivo** para exibir e acessar todos os arquivos de log de auditoria disponíveis no Active IQ Unified Manager. Os arquivos no Audit Log: File View são listados com base em sua data de criação. Esta vista apresenta informações de todo o registro de auditoria que são capturados da instalação ou atualização para o presente no sistema. Sempre que você executa uma ação no Unified Manager, as informações são atualizadas e estão disponíveis nos logs. O status de cada arquivo de log é capturado usando o atributo "Status de integridade de arquivo" que é monitorado ativamente para detectar adulteração ou exclusão do arquivo de log. Os logs de auditoria podem ter um dos seguintes estados quando os logs de auditoria estão disponíveis no sistema:

Estado	Descrição
ATIVO	Ficheiro no qual os registos estão a ser registados atualmente.
NORMAL	Ficheiro inativo, comprimido e armazenado no sistema.
ADULTERADO	Arquivo que foi comprometido por um usuário que editou manualmente o arquivo.
MANUAL_DELETE	Arquivo que foi excluído por um usuário autorizado.
ROLLOVER_DELETE	Ficheiro que foi eliminado devido à implementação com base na política de configuração contínua.
UNEXPECTED_DELETE	Arquivo que foi excluído devido a razões desconhecidas.

A página Registro de auditoria inclui os seguintes botões de comando:

- Configurar
- Eliminar
- Transferir

O botão **DELETE** permite excluir qualquer um dos logs de auditoria listados na exibição Logs de auditoria. Você pode excluir um log de auditoria e, opcionalmente, fornecer um motivo para excluir o arquivo, o que ajudará no futuro a determinar uma exclusão válida. A coluna MOTIVO lista o motivo juntamente com o nome do usuário que realizou a operação de exclusão.



A exclusão de um arquivo de log causará a exclusão do arquivo do sistema, mas a entrada na tabela DB não será excluída.

Você pode baixar os logs de auditoria do Active IQ Unified Manager usando o botão **DOWNLOAD** na seção Logs de auditoria e exportar os arquivos de log de auditoria. Os arquivos marcados como "NORMAL" ou "ADULTERADO" são baixados em um formato compactado .gzip.

Os arquivos de log de auditoria são arquivados periodicamente e salvos no banco de dados para referência. Antes do arquivamento, os logs de auditoria são assinados digitalmente para manter a segurança e a

integridade.

Quando um pacote AutoSupport completo é gerado, o pacote de suporte inclui arquivos de log de auditoria arquivados e ativos. Mas quando um pacote de suporte leve é gerado, ele inclui apenas os logs de auditoria ativos. Os registros de auditoria arquivados não estão incluídos.

### Configurando logs de auditoria

Você pode usar o botão **Configurar** na seção Logs de auditoria para configurar a política de rolagem para arquivos de log de auditoria e também ativar o log remoto para os Logs de auditoria.

Você pode definir os valores nos **DIAS DE RETENÇÃO DO REGISTRO MAX** e **DIAS DE RETENÇÃO DO LOG DE AUDITORIA** de acordo com a quantidade e a frequência desejadas dos dados que deseja armazenar no sistema. O valor no campo **TAMANHO TOTAL DO LOG DE AUDITORIA** é o tamanho dos dados totais do log de auditoria presentes no sistema. A política de rolagem é determinada pelos valores no campo **DIAS DE RETENÇÃO DO LOG DE AUDITORIA**, **TAMANHO DO ARQUIVO MAX** e **TAMANHO TOTAL DO LOG DE AUDITORIA**. Quando o tamanho do backup do log de auditoria atinge o valor configurado em **TAMANHO TOTAL DO LOG DE AUDITORIA**, o arquivo que foi arquivado primeiro é excluído. Isso significa que o arquivo mais antigo é excluído. Mas a entrada de arquivo continua disponível no banco de dados e é marcada como "Rollover Delete". O valor **AUDIT LOG RETENT DAYS** é para o número de dias em que os arquivos de log de auditoria são preservados. Qualquer arquivo mais antigo que o valor definido neste campo é rolado.

#### Passos

1. Clique em **Logs de auditoria > Configurar**.
2. Insira valores em **TAMANHO DO ARQUIVO MAX**, **TAMANHO TOTAL DO LOG DE AUDITORIA** e **DIAS DE RETENÇÃO DO LOG DE AUDITORIA**.

Se pretender ativar o registro remoto, deve selecionar **Ativar registro remoto**.

#### Ativar o registro remoto de registros de auditoria

Pode selecionar a caixa de verificação **Ativar registro remoto** na caixa de diálogo Configurar registros de auditoria para ativar o registro de auditoria remota. Você pode usar esse recurso para transferir logs de auditoria para um servidor Syslog remoto. Isso permitirá que você gerencie seus logs de auditoria quando houver restrições de espaço.

O Registro remoto de logs de auditoria fornece um backup à prova de violação no caso de os arquivos de log de auditoria no servidor Active IQ Unified Manager serem adulterados.

#### Passos

1. Na caixa de diálogo **Configurar registros de auditoria**, selecione a caixa de verificação **Ativar registro remoto**.

São apresentados campos adicionais para configurar o registro remoto.

2. Introduza **HOSTNAME** e **PORT** do servidor remoto ao qual pretende ligar.
3. No campo **CERTIFICADO de CA DO SERVIDOR**, clique em **PROCURAR** para selecionar um certificado público do servidor de destino.

O certificado deve ser carregado em .pem formato. Este certificado deve ser obtido a partir do servidor Syslog de destino e não deve ter expirado. O certificado deve conter o nome do host selecionado como parte do SubjectAltName atributo (SAN).

4. Insira os valores para os seguintes campos: **CHARSET**, **TEMPO LIMITE DE CONEXÃO**, **ATRASO DE CONEXÃO**.

Os valores devem estar em milissegundos para esses campos.

5. Selecione o formato Syslog e a versão do protocolo TLS necessários nos campos **FORMAT** e **PROTOCOL**.
6. Marque a caixa de seleção **Ativar autenticação do cliente** se o servidor Syslog de destino exigir autenticação baseada em certificado.

Você precisará baixar o certificado de autenticação do cliente e enviá-lo para o servidor Syslog antes de salvar a configuração do Log de auditoria, caso contrário a conexão falhará. Dependendo do tipo de servidor Syslog, talvez seja necessário criar um hash do certificado de autenticação do cliente.

Exemplo: O syslog-ng requer que um <hash> do certificado seja criado usando o comando ``openssl x509 -noout -hash -in cert.pem``e, em seguida, você deve vincular simbolicamente o certificado de autenticação do cliente a um arquivo nomeado após o <hash> .0.

7. Clique em **Salvar** para configurar a conexão com o servidor e ativar o Registro remoto.

Você será redirecionado para a página Logs de auditoria.



O valor **tempo limite da conexão** pode afetar a configuração. Se a configuração demorar mais tempo a responder do que o valor definido, pode resultar em falha de configuração devido a um erro de conexão. Para estabelecer uma conexão bem-sucedida, aumente o valor **tempo limite da conexão** e tente a configuração novamente.

## Página Autenticação remota

Você pode usar a página Autenticação remota para configurar o Unified Manager para se comunicar com o servidor de autenticação para autenticar usuários remotos que tentam fazer login na IU da Web do Unified Manager.

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

Depois de selecionar a caixa de verificação Ativar autenticação remota, pode ativar a autenticação remota utilizando um servidor de autenticação.

- **Serviço de autenticação**

Permite configurar o servidor de gerenciamento para autenticar usuários em provedores de serviços de diretório, como Active Directory, OpenLDAP ou especificar seu próprio mecanismo de autenticação. Você só pode especificar um serviço de autenticação se tiver habilitado a autenticação remota.

- **Active Directory**

- Nome do administrador

Especifica o nome de administrador do servidor de autenticação.

- Palavra-passe

Especifica a senha para acessar o servidor de autenticação.

- Nome diferenciado base

Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de [ou@domain.com](#), então o nome distinto base é

- Desative a Pesquisa de grupos aninhados

Especifica se deseja ativar ou desativar a opção de pesquisa de grupo aninhado. Por predefinição, esta opção está desativada. Se você usar o ative Directory, poderá acelerar a autenticação desativando o suporte para grupos aninhados.

- Utilize a ligação segura

Especifica o serviço de autenticação usado para comunicação com servidores de autenticação.

- **OpenLDAP**

- Vincular Nome distinto

Especifica o nome distinto do bind que é usado juntamente com o nome distinto base para encontrar usuários remotos no servidor de autenticação.

- Vincular senha

Especifica a senha para acessar o servidor de autenticação.

- Nome diferenciado base

Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de [ou@domain.com](#), então o nome distinto base é

- Utilize a ligação segura

Especifica que o LDAP seguro é usado para se comunicar com servidores de autenticação LDAP.

- **Outros**

- Vincular Nome distinto

Especifica o nome distinto do bind que é usado juntamente com o nome distinto base para encontrar usuários remotos no servidor de autenticação que você configurou.

- Vincular senha

Especifica a senha para acessar o servidor de autenticação.

- Nome diferenciado base

Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de [ou@domain.com](#), então o nome distinto



base é

- Versão do protocolo

Especifica a versão LDAP (Lightweight Directory Access Protocol) suportada pelo servidor de autenticação. Pode especificar se a versão do protocolo tem de ser detetada automaticamente ou definir a versão para 2 ou 3.

- Atributo Nome Utilizador

Especifica o nome do atributo no servidor de autenticação que contém nomes de login de usuário a serem autenticados pelo servidor de gerenciamento.

- Atributo de associação de grupo

Especifica um valor que atribui a associação do grupo do servidor de gerenciamento a usuários remotos com base em um atributo e valor especificado no servidor de autenticação do usuário.

- UGID

Se os usuários remotos forem incluídos como membros de um objeto GroupOfUniqueNames no servidor de autenticação, essa opção permitirá que você atribua a associação do grupo de servidores de gerenciamento aos usuários remotos com base em um atributo especificado nesse objeto GroupOfUniqueNames.

- Desative a Pesquisa de grupos aninhados

Especifica se deseja ativar ou desativar a opção de pesquisa de grupo aninhado. Por predefinição, esta opção está desativada. Se você usar o ative Directory, poderá acelerar a autenticação desativando o suporte para grupos aninhados.

- Membro

Especifica o nome do atributo que o servidor de autenticação usa para armazenar informações sobre os membros individuais de um grupo.

- Classe Objeto Utilizador

Especifica a classe de objeto de um usuário no servidor de autenticação remota.

- Classe Objeto Grupo

Especifica a classe de objeto de todos os grupos no servidor de autenticação remota.



Os valores que você insere para os atributos *Member*, *User Object Class* e *Group Object Class* devem ser os mesmos que os adicionados nas configurações do ative Directory, OpenLDAP e LDAP. Caso contrário, a autenticação poderá falhar.

- Utilize a ligação segura

Especifica o serviço de autenticação usado para comunicação com servidores de autenticação.



Se pretender modificar o serviço de autenticação, certifique-se de que elimina quaisquer servidores de autenticação existentes e adiciona novos servidores de autenticação.

## Área servidores de autenticação

A área servidores de autenticação exibe os servidores de autenticação com os quais o servidor de gerenciamento se comunica para localizar e autenticar usuários remotos. As credenciais para usuários remotos ou grupos são mantidas pelo servidor de autenticação.

- **Botões de comando**

Permite adicionar, editar ou excluir servidores de autenticação.

- Adicionar

Permite adicionar um servidor de autenticação.

Se o servidor de autenticação que você está adicionando fizer parte de um par de alta disponibilidade (usando o mesmo banco de dados), você também poderá adicionar o servidor de autenticação do parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação está inacessível.

- Editar

Permite editar as definições de um servidor de autenticação selecionado.

- Eliminar

Exclui os servidores de autenticação selecionados.

- **Nome ou endereço IP**

Exibe o nome do host ou o endereço IP do servidor de autenticação usado para autenticar o usuário no servidor de gerenciamento.

- **Porto**

Exibe o número da porta do servidor de autenticação.

- **\* Teste de Autenticação\***

Este botão valida a configuração do servidor de autenticação autenticando um usuário ou grupo remoto.

Durante o teste, se você especificar apenas o nome de usuário, o servidor de gerenciamento pesquisará o usuário remoto no servidor de autenticação, mas não autenticará o usuário. Se especificar o nome de utilizador e a palavra-passe, o servidor de gestão procura e autentica o utilizador remoto.

Não é possível testar a autenticação se a autenticação remota estiver desativada.

## Gerenciamento de certificados de segurança

Você pode configurar o HTTPS no servidor do Unified Manager para monitorar e gerenciar seus clusters em uma conexão segura.

### Exibindo o certificado de segurança HTTPS

Você pode comparar os detalhes do certificado HTTPS com o certificado recuperado em

seu navegador para garantir que a conexão criptografada do navegador com o Unified Manager não esteja sendo interceptada.

#### **Antes de começar**

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

A exibição do certificado permite verificar o conteúdo de um certificado regenerado ou exibir nomes Alt de assunto (SAN) a partir dos quais você pode acessar o Unified Manager.

#### **Passo**

1. No painel de navegação esquerdo, clique em **Geral > certificado HTTPS**.

O certificado HTTPS é exibido na parte superior da página

Se você precisar exibir informações mais detalhadas sobre o certificado de segurança do que as exibidas na página certificado HTTPS, poderá exibir o certificado de conexão no navegador.

### **Transferir uma solicitação de assinatura de certificado HTTPS**

Você pode baixar uma solicitação de assinatura de certificação para o certificado de segurança HTTPS atual para que você possa fornecer o arquivo a uma autoridade de certificação para assinar. Um certificado assinado pela CA ajuda a evitar ataques man-in-the-middle e fornece melhor proteção de segurança do que um certificado autoassinado.

#### **Antes de começar**

Tem de ter a função Administrador de aplicações.

#### **Passos**

1. No painel de navegação esquerdo, clique em **Geral > certificado HTTPS**.
2. Clique em **Download de solicitação de assinatura de certificado HTTPS**.
3. Salve o `<hostname>.csr` arquivo.

Você pode fornecer o arquivo a uma autoridade de certificação para assinar e, em seguida, instalar o certificado assinado.

### **Instalando um certificado HTTPS assinado e retornado pela CA**

Você pode fazer o upload e instalar um certificado de segurança depois que uma Autoridade de certificação o tiver assinado e retornado. O arquivo que você carregar e instalar deve ser uma versão assinada do certificado autoassinado existente. Um certificado assinado pela CA ajuda a evitar ataques man-in-the-middle e fornece melhor proteção de segurança do que um certificado autoassinado.

- O que. Antes de começar

Você deve ter concluído as seguintes ações:

- Fez o download do arquivo de solicitação de assinatura de certificado e o assinou por uma Autoridade de Certificação

- Salva a cadeia de certificados no formato PEM
- Incluídos todos os certificados na cadeia, desde o certificado do servidor Unified Manager até o certificado de assinatura raiz, incluindo quaisquer certificados intermediários presentes

Tem de ter a função Administrador de aplicações.



Se a validade do certificado para o qual um CSR foi criado for superior a 397 dias, a validade será reduzida para 397 dias pela CA antes de assinar e devolver o certificado

### Passos

1. No painel de navegação esquerdo, clique em **Geral > certificado HTTPS**.
2. Clique em **Instalar certificado HTTPS**.
3. Na caixa de diálogo exibida, clique em **escolha arquivo...** para localizar o arquivo a ser carregado.
4. Selecione o arquivo e clique em **Instalar** para instalar o arquivo.

Para obter informações, "[Instalar um certificado HTTPS gerado usando ferramentas externas](#)" consulte .

### Exemplo de cadeia de certificados

O exemplo a seguir mostra como o arquivo de cadeia de certificados pode aparecer:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

### Instalar um certificado HTTPS gerado usando ferramentas externas

Você pode instalar certificados que são autoassinados ou CA assinados e são gerados usando uma ferramenta externa como OpenSSL, BoringSSL, LetsEncrypt.

Você deve carregar a chave privada junto com a cadeia de certificados porque esses certificados são gerados externamente pelo par de chaves público-privadas. Os algoritmos de par de chaves permitidos são "RSA" e "EC". A opção **Instalar certificado HTTPS** está disponível na página certificados HTTPS na seção Geral. O arquivo que você carregar deve estar no seguinte formato de entrada.

1. Chave privada do servidor que pertence ao host Active IQ Unified Manager
2. Certificado do servidor que corresponde à chave privada

3. Certificado das CAs em sentido inverso até a raiz, que são usados para assinar o certificado acima

### Formato para carregar um certificado com um par de chaves EC

As curvas permitidas são "prime256v1" e "ecp384r1". Amostra de certificado com um par EC gerado externamente:

```
-----BEGIN EC PRIVATE KEY-----  
<EC private key of Server>  
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----  
<Server certificate>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Intermediate certificate #1 (if present)>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Intermediate certificate #2 (if present)>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Root signing certificate>  
-----END CERTIFICATE-----
```

### Formato para carregar um certificado com um par de chaves RSA

Os tamanhos de chave permitidos para o par de chaves RSA pertencentes ao certificado de host são 2048, 3072 e 4096. Certificado com um par de chaves **RSA gerado externamente**:

```
-----BEGIN RSA PRIVATE KEY-----  
<RSA private key of Server>  
-----END RSA PRIVATE KEY-----  
-----BEGIN CERTIFICATE-----  
<Server certificate>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Intermediate certificate #1 (if present)>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Intermediate certificate #2 (if present)>  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
<Root signing certificate>  
-----END CERTIFICATE-----
```

Depois que o certificado for carregado, você deverá reiniciar a instância do Active IQ Unified Manager para que as alterações entrem em vigor.

### Verifica durante o carregamento de certificados gerados externamente

O sistema executa verificações ao carregar um certificado gerado usando ferramentas externas. Se alguma das verificações falhar, o certificado será rejeitado. Há também validação incluída para os certificados que são gerados a partir do CSR dentro do produto e para os certificados que são gerados usando ferramentas externas.

- A chave privada na entrada é validada com base no certificado do host na entrada.
- O Nome Comum (CN) no certificado de host é verificado em relação ao FQDN do host.
- O Nome Comum (CN) do certificado de anfitrião não deve estar vazio ou em branco e não deve ser definido como localhost.
- A data de início da validade não deve ser futura e a data de validade do certificado não deve ser anterior.
- Se houver CA ou CA intermediária, a data de início de validade do certificado não deve ser no futuro e a data de validade não deve ser no passado.



A chave privada na entrada não deve ser criptografada. Se houver chaves privadas criptografadas, elas serão rejeitadas pelo sistema.

#### Exemplo 1

```
-----BEGIN ENCRYPTED PRIVATE KEY-----  
<Encrypted private key>  
-----END ENCRYPTED PRIVATE KEY-----
```

#### Exemplo 2

```
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
<content here>  
-----END RSA PRIVATE KEY-----
```

#### Exemplo 3

```
-----BEGIN EC PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
<content here>  
-----END EC PRIVATE KEY-----
```

Se a instalação do certificado falhar, consulte o artigo da base de conhecimento (KB): ["O ActiveIQ Unified Manager não instala um certificado gerado externamente"](#)

## Descrições de páginas para gerenciamento de certificados

Você pode usar a página certificado HTTPS para exibir os certificados de segurança atuais e gerar novos certificados HTTPS.

### Página certificado HTTPS

A página certificado HTTPS permite exibir o certificado de segurança atual, fazer download de uma solicitação de assinatura de certificado, gerar um novo certificado HTTPS autoassinado ou instalar um novo certificado HTTPS.

Se não tiver gerado um novo certificado HTTPS auto-assinado, o certificado que aparece nesta página é o certificado que foi gerado durante a instalação.

#### Botões de comando

Os botões de comando permitem executar as seguintes operações:

- \* Faça o download do pedido de assinatura de certificado HTTPS\*

Transfere uma solicitação de certificação para o certificado HTTPS atualmente instalado. O navegador solicita que você salve o arquivo <hostname>.csr para que você possa fornecer o arquivo a uma autoridade de certificação para assinar.

- **Instalar certificado HTTPS**

Permite que você carregue e instale um certificado de segurança depois que uma autoridade de certificação o tiver assinado e devolvido. O novo certificado entra em vigor após reiniciar o servidor de gerenciamento.

- **Regenerate HTTPS Certificate**

Permite gerar um novo certificado HTTPS autoassinado, que substitui o certificado de segurança atual. O novo certificado entrará em vigor após a reinicialização do Unified Manager.

### Caixa de diálogo regenerar certificado HTTPS

A caixa de diálogo regenerar certificado HTTPS permite personalizar as informações de segurança e, em seguida, gerar um novo certificado HTTPS com essas informações.

As informações atuais do certificado são exibidas nesta página.

A seleção ""regenerar usando atributos de certificado atuais"" e ""Atualizar os atributos de certificado atuais"" permite que você regenere o certificado com as informações atuais ou gere um certificado com novas informações.

- **Nome comum**

Obrigatório. O nome de domínio totalmente qualificado (FQDN) que você deseja proteger.

Nas configurações de alta disponibilidade do Unified Manager, use o endereço IP virtual.

- **Email**

Opcional. Um endereço de e-mail para entrar em Contato com sua organização; normalmente, o endereço de e-mail do administrador de certificados ou do departamento DE TI.

- **Empresa**

Opcional. Normalmente, o nome incorporado da sua empresa.

- **Departamento**

Opcional. O nome do departamento em sua empresa.

- **Cidade**

Opcional. A localização da cidade da sua empresa.

- **Estado**

Opcional. A localização do estado ou da província, não abreviada, da sua empresa.

- **País**

Opcional. A localização do país da sua empresa. Este é normalmente um código ISO de duas letras do país.

- **Nomes alternativos**

Obrigatório. Nomes de domínio adicionais não primários que podem ser usados para acessar este servidor, além do localhost existente ou outros endereços de rede. Separe cada nome alternativo com uma vírgula.

Marque a caixa de seleção "Excluir informações de identificação local (por exemplo, localhost)" se quiser remover as informações de identificação local do campo nomes alternativos no certificado. Quando esta caixa de verificação está selecionada, apenas o que introduzir no campo é utilizado no campo nomes alternativos. Quando deixado em branco, o certificado resultante não terá um campo de nomes alternativos.

- \* TAMANHO DA CHAVE (ALGORITMO DE CHAVE: RSA)\*

O algoritmo de chave é definido como RSA. Você pode selecionar um dos tamanhos de chave: 2048, 3072 ou 4096 bits. O tamanho da chave padrão é definido para 2048 bits.

- **PERÍODO DE VALIDADE**

O período de validade padrão é de 397 dias. Se você tiver atualizado de uma versão anterior, poderá ver a validade do certificado anterior inalterada.

Para obter mais informações, ["Gerando certificados HTTPS"](#) consulte .



# Monitorar e gerenciar o storage

## Introdução ao Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente chamado Gerenciador Unificado de OnCommand) permite que você monitore e gerencie a integridade e a performance dos sistemas de storage da ONTAP com uma única interface.

O Unified Manager oferece os seguintes recursos:

- Detecção, monitoramento e notificações de sistemas instalados com o software ONTAP.
- Painel para mostrar a capacidade, segurança e integridade de performance do ambiente.
- Infraestrutura de alertas, eventos e limites aprimorados.
- Exibe gráficos detalhados que plotam a atividade do workload ao longo do tempo, incluindo IOPS (operações), Mbps (taxa de transferência), latência (tempo de resposta), utilização, capacidade de performance e taxa de cache.
- Identifica cargas de trabalho que estão sobreusando componentes do cluster e as cargas de trabalho cujo desempenho é afetado pelo aumento da atividade.
- Fornece ações corretivas sugeridas que podem ser executadas para resolver certos incidentes e eventos, e um botão "corrigir" para alguns eventos para que você possa resolver o problema imediatamente.
- Integra-se ao OnCommand Workflow Automation para executar fluxos de trabalho de proteção automatizada.
- Capacidade de criar novos workloads, como um LUN ou compartilhamento de arquivos, diretamente do Unified Manager e atribuir um nível de Serviço de Performance para definir os objetivos de desempenho e storage para os usuários que acessam a aplicação usando esse workload.

## Introdução ao monitoramento da saúde do Active IQ Unified Manager

O Active IQ Unified Manager (antigo Gerenciador Unificado de OnCommand) ajuda você a monitorar um grande número de sistemas que executam o software ONTAP por meio de uma interface de usuário centralizada. A infraestrutura de servidor do Unified Manager oferece escalabilidade, capacidade de suporte e recursos aprimorados de monitoramento e notificação.

Os principais recursos do Unified Manager incluem monitoramento, alerta, gerenciamento de disponibilidade e capacidade dos clusters, gerenciamento de recursos de proteção e agrupamento de dados de diagnóstico e envio para o suporte técnico.

Você pode usar o Unified Manager para monitorar os clusters. Quando ocorrem problemas no cluster, o Unified Manager notifica você sobre os detalhes de tais problemas por meio de eventos. Alguns eventos também fornecem uma ação corretiva que você pode tomar para corrigir os problemas. Você pode configurar alertas para eventos para que, quando os problemas ocorrem, você seja notificado por e-mail e traps SNMP.

Você pode usar o Unified Manager para gerenciar objetos de storage em seu ambiente associando-os a anotações. Você pode criar anotações personalizadas e associar dinamicamente clusters, máquinas virtuais de armazenamento (SVMs) e volumes às anotações por meio de regras.

Você também pode Planejar os requisitos de armazenamento dos objetos de cluster usando as informações

fornecidas nos gráficos de capacidade e integridade para o respectivo objeto de cluster.

## Capacidade física e lógica

O Unified Manager faz uso dos conceitos de espaço físico e lógico usados para objetos de storage do ONTAP.

- Capacidade física: O espaço físico refere-se aos blocos físicos de armazenamento utilizados no volume. "Capacidade física usada" geralmente é menor que a capacidade lógica usada devido à redução de dados de recursos de eficiência de storage (como deduplicação e compactação).
- Capacidade lógica: O espaço lógico refere-se ao espaço utilizável (os blocos lógicos) em um volume. O espaço lógico refere-se a como o espaço teórico pode ser usado, sem levar em conta os resultados da deduplicação ou compressão. "Espaço lógico usado" é o espaço físico usado, além da economia com recursos de eficiência de storage (como deduplicação e compactação) que foram configurados. Essa medida geralmente parece maior do que a capacidade física usada, pois isso não reflete a compressão de dados e outras reduções no espaço físico. Assim, a capacidade lógica total poderia ser maior do que o espaço provisionado.

## Unidades de medição da capacidade

O Unified Manager calcula a capacidade de armazenamento com base em unidades binárias de 1024 (2,10) bytes. No ONTAP 9.10,0 e anterior, essas unidades foram exibidas como KB, MB, GB, TB e PB. A partir do ONTAP 9.10,1, eles são exibidos no Gerenciador Unificado como KiB, MiB, GiB, TiB e PiB.



As unidades usadas para a taxa de transferência continuam a ser kilobytes por segundo (Kbps), megabytes por segundo (Mbps), Gigabytes por segundo (Gbps) ou Terabytes por segundo (Tbps) e assim por diante, para todas as versões do ONTAP.

Unidade de capacidade exibida no Gerenciador Unificado para ONTAP 9.10,0 e anterior	Unidade de capacidade exibida no Gerenciador Unificado para o ONTAP 9.10,1	Cálculo	Valor em bytes
KB	KiB	1024	1024 bytes
MB	MiB	1024 * 1024	1.048.576 bytes
GB	GiB	1024 * 1024 * 1024	1.073.741.824 bytes
TB	TiB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 bytes

## Introdução ao monitoramento de desempenho do Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente chamado Gerenciador Unificado de OnCommand) fornece recursos de monitoramento de desempenho e análise de causa-raiz de eventos para sistemas que executam o software NetApp ONTAP.

O Unified Manager ajuda você a identificar workloads que estão sobrecarregando componentes do cluster e diminuindo o desempenho de outros workloads no cluster. Ao definir políticas de limite de desempenho, você também pode especificar valores máximos para determinados contadores de desempenho para que os eventos sejam gerados quando o limite for violado. O Unified Manager alerta você sobre esses eventos de

performance para que você tome medidas corretivas e coloque a performance de volta ao nível normal de operação. Você pode exibir e analisar eventos na IU do Unified Manager.

O Unified Manager monitora a performance de dois tipos de workloads:

- Workloads definidos pelo usuário

Esses workloads consistem em FlexVol volumes e FlexGroup volumes criados no cluster.

- Workloads definidos pelo sistema

Esses workloads consistem em atividade interna do sistema.

## Usando APIs REST do Unified Manager

O Active IQ Unified Manager fornece APIs REST para você visualizar informações sobre monitoramento e gerenciamento do ambiente de storage. As APIs também permitem provisionar e gerenciar objetos de storage com base em políticas.

Você também pode executar APIs do ONTAP em todos os clusters gerenciados pelo ONTAP usando o gateway de API compatível com o Unified Manager.

Para obter informações sobre as APIs REST do Unified Manager, "[Primeiros passos com as APIs REST do Active IQ Unified Manager](#)" consulte .

## O que o servidor Unified Manager faz

A infraestrutura de servidor do Unified Manager consiste em uma unidade de coleta de dados, um banco de dados e um servidor de aplicativos. Ele fornece serviços de infraestrutura como descoberta, monitoramento, controle de acesso baseado em funções (RBAC), auditoria e logs.

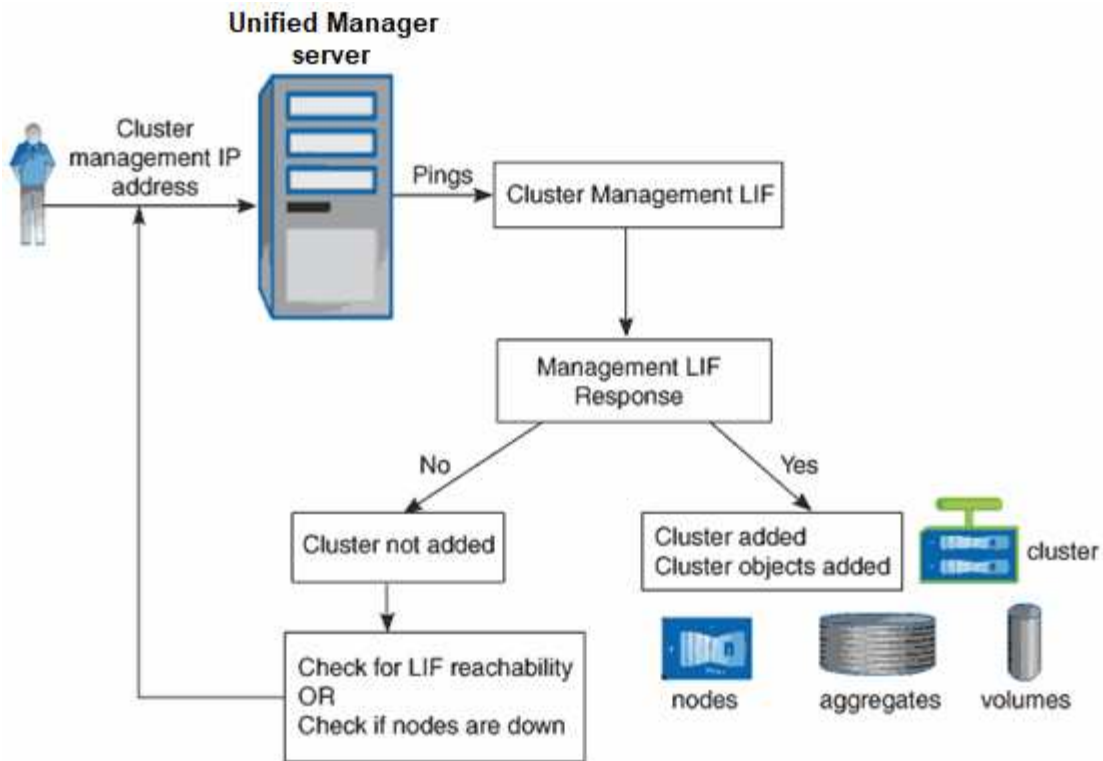
O Unified Manager coleta informações de cluster, armazena os dados no banco de dados e analisa os dados para verificar se há problemas de cluster.

### Como funciona o processo de descoberta

Depois de adicionar o cluster ao Unified Manager, o servidor descobre os objetos do cluster e os adiciona ao banco de dados. Entender como funciona o processo de descoberta ajuda você a gerenciar os clusters da sua organização e seus objetos.

O intervalo de monitoramento padrão é de 15 minutos: Se você tiver adicionado um cluster ao servidor do Unified Manager, levará 15 minutos para exibir os detalhes do cluster na IU do Unified Manager.

A imagem a seguir ilustra o processo de descoberta no Active IQ Unified Manager:



## Compreender a interface do utilizador

A interface de usuário do Unified Manager consiste principalmente em um painel que fornece uma visualização rápida dos objetos monitorados. A interface do usuário também fornece acesso à visualização de todos os objetos do cluster.

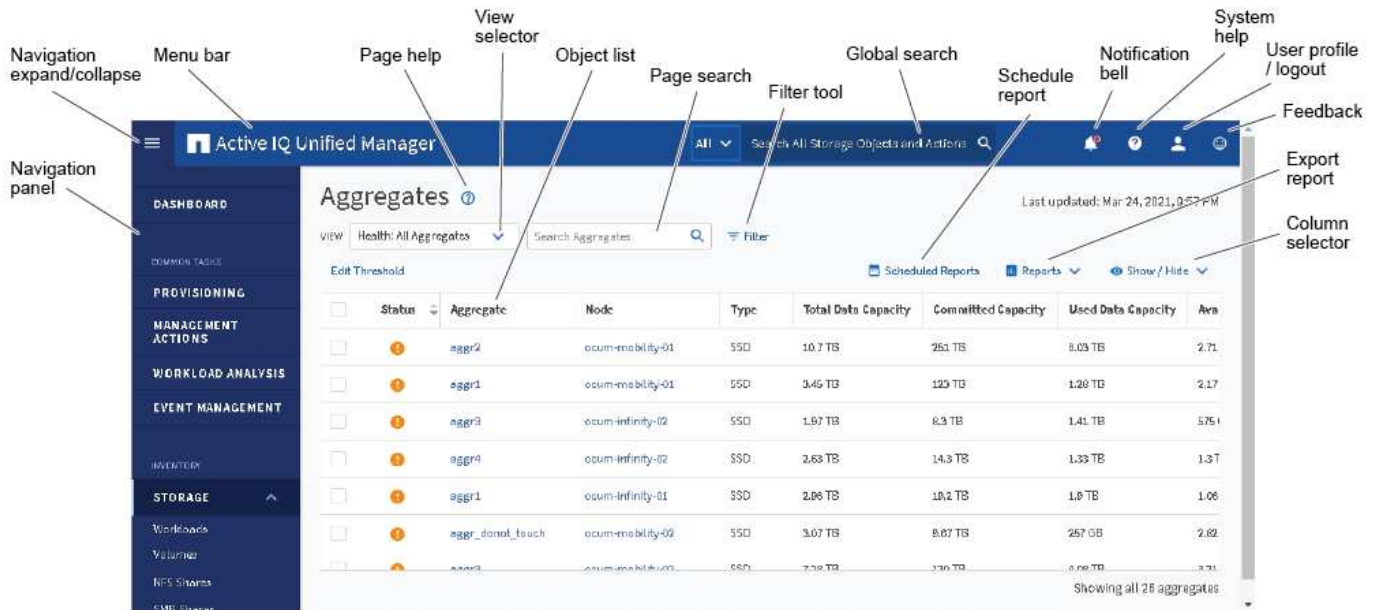
Pode selecionar uma vista preferida e utilizar os botões de ação, conforme necessário. A configuração da tela é salva em um espaço de trabalho para que toda a funcionalidade necessária esteja disponível quando você iniciar o Unified Manager. No entanto, quando você navega de uma exibição para outra e, em seguida, navega para trás, a exibição pode não ser a mesma.

### Layouts de janela típicos

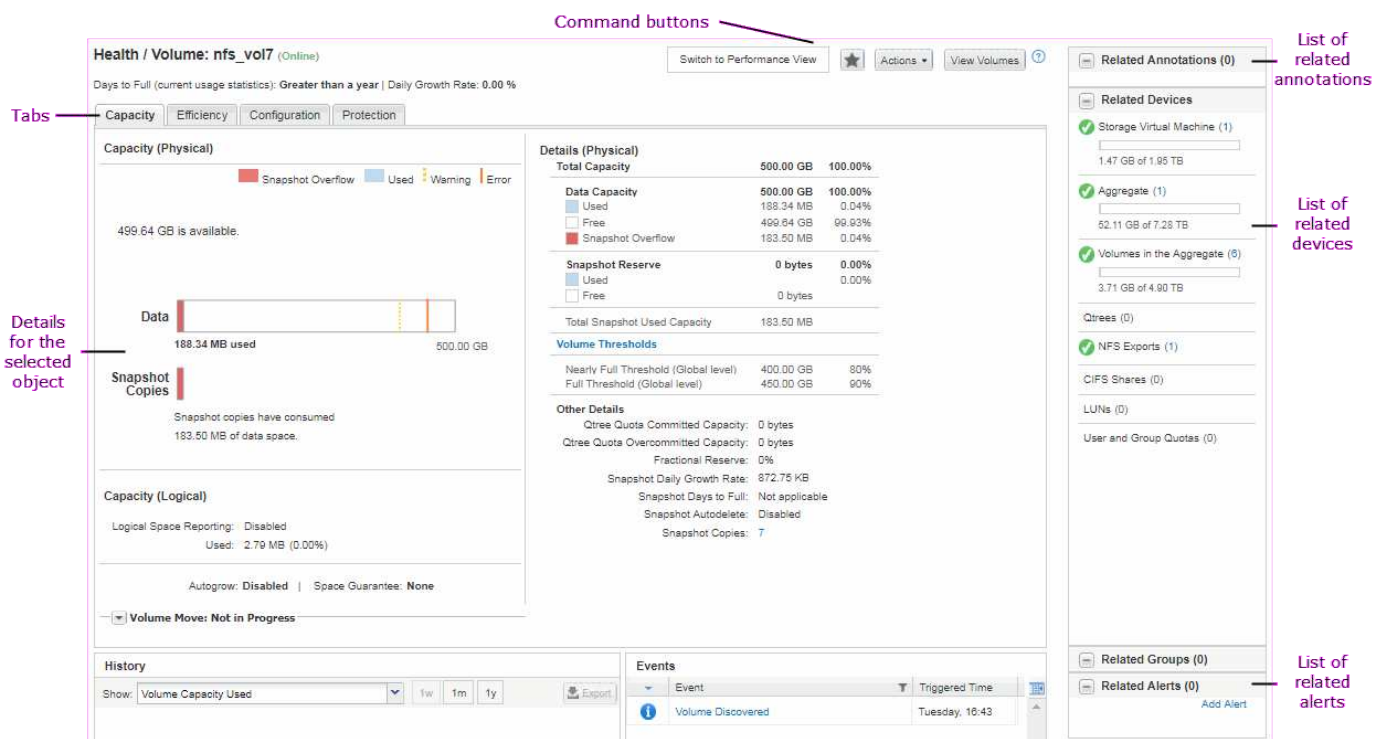
Entender os layouts típicos de janelas ajuda você a navegar e usar o Active IQ Unified Manager de forma eficaz. A maioria das janelas do Unified Manager é semelhante a um dos dois layouts gerais: Lista de objetos ou detalhes. A configuração de exibição recomendada é de pelo menos 1280 por 1024 pixels.

Nem todas as janelas contêm todos os elementos nos diagramas a seguir.

#### Layout da janela da lista de objetos



## Layout da janela de detalhes do objeto



## Personalização do layout da janela


O Active IQ Unified Manager permite personalizar o layout das informações nas páginas de objetos de armazenamento e rede. Ao personalizar as janelas, pode controlar quais os dados que podem ser visualizados e como os dados são apresentados.

- **Classificação**

Você pode clicar no cabeçalho da coluna para alterar a ordem de classificação das entradas da coluna.

Quando você clica no cabeçalho da coluna, as setas de classificação (▲ e ▼) aparecem para essa coluna.

- **Filtragem**

Você pode clicar no ícone de filtro () para aplicar filtros para personalizar a exibição de informações nas páginas de objetos de armazenamento e rede, de modo que somente as entradas que correspondem às condições fornecidas sejam exibidas. Você aplica filtros do painel filtros.

O painel filtros permite filtrar a maioria das colunas com base nas opções selecionadas. Por exemplo, na exibição Saúde: Todos os volumes, você pode usar o painel filtros para exibir todos os volumes offline selecionando a opção de filtro apropriada em Estado.

Colunas relacionadas à capacidade em qualquer lista sempre exibem dados de capacidade em unidades apropriadas arredondadas para dois pontos decimais. Isso também se aplica ao filtrar colunas de capacidade. Por exemplo, se você usar o filtro na coluna capacidade total de dados na exibição Saúde: Todos os agregados para filtrar dados acima de 20,45 GB, a capacidade real de 20,454 GB será exibida como 20,45 GB. Da mesma forma, se você filtrar dados com menos de 20,45 GB, a capacidade real de 20,449 GB será exibida como 20,45 GB.

Se você usar o filtro na coluna % de dados disponíveis na visualização Saúde: Todos os agregados para filtrar dados acima de 20,45%, a capacidade real de 20,454% será exibida como 20,45%. Da mesma forma, se você filtrar dados menos de 20,45%, a capacidade real de 20,449% será exibida como 20,45%.

- **Ocultando ou mostrando as colunas**

Você pode clicar no ícone de exibição de coluna (**Mostrar/Ocultar**) para selecionar quais colunas deseja exibir. Depois de selecionar as colunas apropriadas, você pode reordená-las arrastando-as usando o Mouse.

- **A pesquisar**

Você pode usar a caixa de pesquisa para pesquisar determinados atributos de objeto para ajudar a refinar a lista de itens na página de inventário. Por exemplo, você pode inserir "nuvem" para refinar a lista de volumes na página de inventário de volumes para ver todos os volumes que têm a palavra "nuvem" neles.

- \* Exportação de dados\*


Você pode clicar no botão **relatórios** (ou no botão **Exportar** para exportar dados para um arquivo de valores separados por vírgulas (.csv), (.pdf) documento ou arquivo do Microsoft Excel (.xlsx) e usar os dados exportados para criar relatórios.


## Usando a Ajuda do Unified Manager

A Ajuda inclui informações sobre todos os recursos incluídos no Active IQ Unified Manager. Você pode usar o índice, o índice ou a ferramenta de pesquisa para encontrar informações sobre os recursos e como usá-los.

A ajuda está disponível em cada guia e na barra de menus da interface do usuário do Unified Manager.

A ferramenta de pesquisa na Ajuda não funciona para palavras parciais.

- Para saber mais sobre campos ou parâmetros específicos, clique  em .

- Para visualizar todo o conteúdo da Ajuda, clique em  \* > \*Ajuda/Documentação na barra de menus.  
Você pode encontrar informações mais detalhadas expandindo qualquer parte do conteúdo no painel de navegação.
- Para pesquisar o conteúdo da Ajuda, clique na guia **pesquisar** no painel de navegação, digite a palavra ou série de palavras que deseja localizar e clique em **ir!**
- Para imprimir tópicos da Ajuda, clique no ícone da impressora.

## Marcar os seus tópicos de Ajuda favoritos

Na guia Favoritos da Ajuda, você pode marcar os tópicos da Ajuda que você usa com frequência. Os marcadores de ajuda fornecem acesso rápido aos seus tópicos favoritos.

### Passos

1. Navegue até o tópico Ajuda que você deseja adicionar como favorito.
2. Clique em **Favoritos** e, em seguida, clique em **Adicionar**.

## A procurar objetos de armazenamento

Para acessar rapidamente um objeto específico, você pode usar o campo **pesquisar todos os objetos de armazenamento** na parte superior da barra de menus. Este método de pesquisa global em todos os objetos permite localizar rapidamente objetos específicos por tipo. Os resultados da pesquisa são classificados por tipo de objeto de armazenamento e você pode filtrá-los ainda mais por objeto usando o menu suspenso.

### Antes de começar

- Você deve ter uma das seguintes funções para executar esta tarefa: Operador, Administrador de aplicativos ou Administrador de armazenamento.
- Uma pesquisa válida deve conter pelo menos três caracteres.

Ao usar o valor do menu suspenso "All", a pesquisa global exibe o número total de resultados encontrados em todas as categorias de objetos; com um máximo de 25 resultados de pesquisa para cada categoria de objeto. Você pode selecionar um tipo de objeto específico no menu suspenso para refinar a pesquisa dentro de um tipo de objeto específico. Neste caso, a lista retornada não está restrita aos 25 principais objetos.

Os tipos de objeto que você pode pesquisar incluem:

- Clusters
- Nós
- VMs de storage
- Agregados
- Volumes
- Qtrees
- Compartilhamentos SMB
- Compartilhamentos de NFS
- Quotas de utilizador ou de grupo

- LUNs
- Namespaces NVMe
- Grupos de iniciadores
- Iniciadores
- Grupo de consistência

A inserção de um nome de workload retorna a lista de workloads na categoria de volumes ou LUNs apropriados.

Você pode clicar em qualquer objeto nos resultados da pesquisa para navegar para a página de detalhes de integridade desse objeto. Se não houver uma página de integridade direta para um objeto, a página Saúde do objeto pai será exibida. Por exemplo, ao pesquisar um LUN específico, a página de detalhes do SVM na qual o LUN reside é exibida.

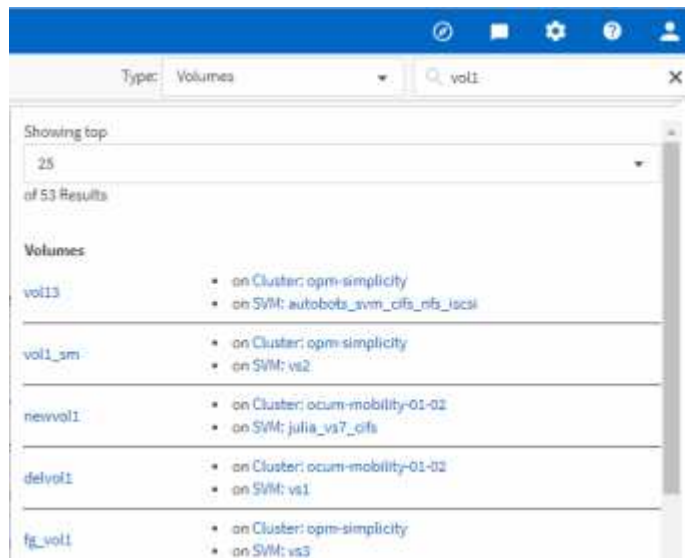


Portas e LIFs não são pesquisáveis na barra de pesquisa global.

## Passos

1. Selecione um tipo de objeto no menu para refinar os resultados da pesquisa para apenas um único tipo de objeto.
2. Digite um mínimo de três caracteres do nome do objeto no campo **pesquisar todos os objetos de armazenamento**.

Neste exemplo, a caixa suspensa tem o tipo de objeto volumes selecionado. Digitar "vol1" no campo **pesquisar todos os objetos de armazenamento** exibe uma lista de todos os volumes cujos nomes contêm esses caracteres.



## Exportar dados de armazenamento como relatórios

Você pode exportar dados de armazenamento em vários formatos de saída e, em seguida, usar os dados exportados para criar relatórios. Por exemplo, se houver 10 eventos críticos que não foram resolvidos, você poderá exportar os dados da página de inventário do Gerenciamento de Eventos para criar um relatório e, em seguida, enviar o relatório para administradores que podem resolver os problemas.



Você pode exportar dados para um `.csv` arquivo, `.xlsx` arquivo ou `.pdf` documento das páginas de inventário **armazenamento** e **rede** e usar os dados exportados para criar relatórios. Existem outros locais no produto onde apenas `.csv` ou `.pdf` arquivos podem ser gerados.

## Passos

1. Execute uma das seguintes ações:

Se você quiser exportar...	Faça isso...
Detalhes do inventário de objetos de armazenamento	Clique em <b>Storage</b> ou <b>Network</b> no menu de navegação à esquerda e selecione um objeto de armazenamento. Escolha uma das exibições fornecidas pelo sistema ou qualquer exibição personalizada que você tenha criado.
Detalhes do grupo de política de QoS	Clique em <b>Storage &gt; QoS Policy Groups</b> no menu de navegação à esquerda.
Detalhes do histórico de proteção e capacidade de armazenamento	Clique em <b>armazenamento &gt; agregados</b> ou <b>armazenamento &gt; volumes</b> e selecione um único agregado ou volume.
Detalhes do evento	Clique em <b>Gerenciamento de eventos</b> no menu de navegação à esquerda.
Os 10 melhores detalhes de desempenho do objeto de storage	Clique em <b>Storage &gt; clusters &gt; Performance:All clusters</b> , selecione um cluster e escolha a guia <b>Top Performers</b> . Em seguida, selecione um objeto de armazenamento e contador de desempenho.

2. Clique no botão **relatórios** (ou no botão **Exportar** em algumas páginas da IU).
3. Clique em **Download CSV**, **Download PDF** ou **Download Excel** para confirmar a solicitação de exportação.

Na guia principais executores, você pode optar por baixar um relatório das estatísticas para o único cluster que você está visualizando ou para todos os clusters no data center.

O ficheiro é transferido.

4. Abra o arquivo no aplicativo apropriado.

## Informações relacionadas

["Página de inventário de integridade/clusters"](#)

["Agendar um relatório"](#)

## Filtrando o conteúdo da página de inventário

Você pode filtrar os dados da página de inventário no Unified Manager para localizar rapidamente os dados com base em critérios específicos. Você pode usar a filtragem

para restringir o conteúdo das páginas do Unified Manager para mostrar apenas os resultados nos quais você está interessado. Isso fornece um método muito eficiente de exibir apenas os dados nos quais você está interessado.

Use **Filtering** para personalizar a exibição de grade com base em suas preferências. As opções de filtro disponíveis são baseadas no tipo de objeto que está sendo visualizado na grade. Se os filtros forem aplicados atualmente, o número de filtros aplicados será exibido à direita do botão filtro.

Três tipos de parâmetros de filtro são suportados.

Parâmetro	Validação
Cadeia de caracteres (texto)	Os operadores são <b>contém, começa com, termina com e não contém</b> .
Número	Os operadores são <b>maiores que, menos que, no último e entre</b> .
Enum (texto)	Os operadores são <b>is e não</b> .

Os campos coluna, Operador e valor são necessários para cada filtro; os filtros disponíveis refletem as colunas filtráveis na página atual. O número máximo de filtros que você pode aplicar é de quatro. Os resultados filtrados são baseados em parâmetros de filtro combinados. Os resultados filtrados aplicam-se a todas as páginas da pesquisa filtrada, não apenas à página exibida atualmente.

Você pode adicionar filtros usando o painel filtragem.

1. Na parte superior da página, clique no botão **filtro**. O painel filtragem é exibido.
2. Clique na lista suspensa esquerda e selecione um objeto; por exemplo, *Cluster* ou um contador de desempenho.
3. Clique na lista pendente central e selecione o operador que pretende utilizar.
4. Na última lista, selecione ou insira um valor para concluir o filtro para esse objeto.
5. Para adicionar outro filtro, clique em *\* Adicionar filtro\**. É apresentado um campo de filtro adicional. Conclua este filtro usando o processo descrito nas etapas anteriores. Observe que ao adicionar seu quarto filtro, o botão *\* Adicionar filtro \** não é mais exibido.
6. Clique em **Apply Filter** (aplicar filtro). As opções de filtro são aplicadas à grade e o número de filtros é exibido à direita do botão filtro.
7. Use o painel filtragem para remover filtros individuais clicando no ícone de lixo à direita do filtro a ser removido.
8. Para remover todos os filtros, clique em **Reset** na parte inferior do painel de filtragem.

### Exemplo de filtragem

A ilustração mostra o painel filtragem com três filtros. O botão *\* Adicionar filtro \** é exibido quando você tem menos do que o máximo de quatro filtros.

MBps	greater than	5	MBps	
Node	name starts with	test		
Type	is	FCP Port		
<input type="button" value="+ Add Filter"/>				
				<input type="button" value="Cancel"/> <input type="button" value="Apply Filter"/>

Depois de clicar em **Apply Filter**, o painel Filtering fecha, aplica os filtros e mostra o número de filtros aplicados ( 3 ).

## Ver eventos ativos a partir do sino de notificação

O sino de notificação ( ) na barra de menus fornece uma maneira rápida de exibir os eventos ativos mais importantes que o Unified Manager está rastreando.

A lista de eventos ativos fornece uma maneira de ver o número total de eventos críticos, de erro, de aviso e de atualização em todos os clusters. Esta lista inclui eventos dos últimos 7 dias e não inclui eventos de Informação. Você pode clicar em um link para exibir a lista de eventos nos quais você está mais interessado.

Observe que quando um cluster não é acessível, o Unified Manager exibe essas informações nesta página. Você pode visualizar informações detalhadas sobre um cluster que não é acessível clicando no botão **Detalhes**. Esta ação abre a página de detalhes do evento. Problemas de monitoramento de escala, como baixo espaço ou RAM na estação de gerenciamento, também são exibidos nesta página.

### Passos

1. Na barra de menus, clique em .
2. Para ver detalhes de qualquer um dos eventos ativos, clique no link de texto do evento, como "capacidade 2" ou "desempenho 4".

## Monitoramento e gerenciamento de clusters no painel

O painel fornece informações gerais cumulativas sobre a integridade atual dos sistemas ONTAP monitorados. O dashboard fornece "painéis" que permitem avaliar a capacidade geral, o desempenho e a integridade da segurança dos clusters que você está monitorando.

Além disso, há certos problemas do ONTAP que você pode corrigir diretamente na interface de usuário do Unified Manager em vez de usar o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

Na parte superior do painel, você pode selecionar se os painéis mostram informações para todos os clusters monitorados ou para um cluster individual. Você pode começar visualizando o status de todos os clusters e, em seguida, pesquisar clusters individuais quando quiser exibir informações detalhadas.



Alguns dos painéis listados abaixo podem não aparecer na página com base na sua configuração.

<b>Painéis</b>	<b>Descrição</b>
Ações de gerenciamento	Quando o Unified Manager pode diagnosticar e determinar uma única resolução para um problema, essas resoluções são exibidas neste painel com um botão <b>Fix it</b> .
Capacidade	Exibe a capacidade total e usada da camada local e da camada de nuvem e o número de dias até a capacidade local atingir o limite superior.
Capacidade de performance	Exibe o valor da capacidade de desempenho de cada cluster e o número de dias até que a capacidade de desempenho atinja o limite superior.
IOPS	Exibe o número total de workloads que estão atualmente em execução em um determinado intervalo de IOPS.
Performance de workload	Exibe o número total de workloads em conformidade e não conformes que são atribuídos a cada nível de Serviço de Performance definido.
Segurança	Exibe o número de clusters compatíveis ou não compatíveis, o número de SVMs em conformidade ou não compatíveis e o número de volumes criptografados ou não criptografados.
Proteção	Exibe o número de VMs de storage protegidas pela relação SVM-DR, volumes protegidos pela relação SnapMirror, volumes protegidos por Snapshot e clusters protegidos pela MetroCluster.
Visão geral de uso	Exibe clusters classificados por IOPS mais alto, maior taxa de transferência (Mbps) ou maior capacidade física usada.

## **Página do painel de instrumentos**

A página Dashboard tem "painéis" que exibem a capacidade, o desempenho e a integridade de segurança de alto nível dos clusters que você está monitorando. Esta página também fornece um painel ações de gerenciamento que lista as correções que o Unified Manager pode fazer para resolver determinados eventos.

A maioria dos painéis também exibe o número de eventos ativos nessa categoria e o número de novos eventos adicionados nas 24 horas anteriores. Essas informações ajudam você a decidir quais clusters você pode precisar analisar mais para resolver eventos. Clicar nos eventos exibe os principais eventos e fornece um link para a página de inventário do Gerenciamento de Eventos filtrada para mostrar os eventos ativos nessa categoria.

Na parte superior do painel, você pode selecionar se os painéis mostram informações para todos os clusters monitorados ("todos os clusters") ou para um cluster individual. Você pode começar visualizando o status de todos os clusters e, em seguida, pesquisar clusters individuais quando quiser exibir informações detalhadas.



Alguns dos painéis listados abaixo aparecem no painel com base na sua configuração.

### **Painel ações de gerenciamento**

Há certos problemas que o Unified Manager faz o diagnóstico completo e fornece uma única resolução. Quando disponíveis, essas resoluções são exibidas neste painel com um botão **Fix it** ou **Fix All**. Você pode corrigir esses problemas imediatamente a partir do Unified Manager em vez de usar o ONTAP System Manager ou a CLI do ONTAP. Para visualizar todos os problemas, clique em consulte ["Correção de problemas do ONTAP diretamente do Unified Manager"](#) para obter mais informações.

### **Painel de capacidade**

Ao visualizar todos os clusters, esse painel exibe a capacidade física usada (depois de aplicar a economia de eficiência de storage) e a capacidade física disponível (não incluindo a possível economia em eficiência de storage) para cada cluster, o número de dias até que os discos estejam cheios e a taxa de redução de dados (sem cópias Snapshot) com base nas configurações de eficiência de storage da ONTAP configuradas. Ele também lista a capacidade usada para todas as categorias de nuvem configuradas. Clicar no gráfico de barras leva você à página de inventário de agregados para esse cluster. Ao clicar no texto "dias até completo", você exibe uma mensagem que identifica o agregado com o menor número de dias de capacidade restantes; clique no nome do agregado para ver mais detalhes.

Ao exibir um único cluster, esse painel exibe a capacidade física usada e a capacidade física disponível para os agregados de dados classificados por cada tipo de disco individual na camada local e para a camada de nuvem. Clicar no gráfico de barras para um tipo de disco leva você à página de inventário de volumes para os volumes que usam esse tipo de disco.

### **Painel capacidade de desempenho**

Ao visualizar todos os clusters, esse painel exibe o valor da capacidade de desempenho para cada cluster (média sobre as 1 horas anteriores) e o número de dias até que a capacidade de desempenho atinja o limite superior (com base na taxa de crescimento diária). Clicar no gráfico de barras leva você à página de inventário de nós para esse cluster. Observe que a página de inventário de nós exibe a média da capacidade de desempenho nas 72 horas anteriores. Ao clicar no texto "dias até completo", você exibe uma mensagem que identifica o nó com o menor número de dias de capacidade de desempenho restantes; clique no nome do nó para ver mais detalhes.

Ao exibir um único cluster, esse painel exibe os valores de porcentagem de capacidade de desempenho do cluster usada, IOPS total e taxa de transferência total (MB/s) e o número de dias até que cada uma dessas três métricas atinja seu limite superior.

### **Painel IOPS do workload**

Ao exibir um único cluster, esse painel exibe o número total de cargas de trabalho atualmente em execução em um determinado intervalo de IOPS e indica o número de cada tipo de disco quando você passa o cursor sobre o gráfico.

### **Painel Performance do workload**

Esse painel exibe o número total de workloads em conformidade e não conformes atribuídos a cada política de nível de serviço de desempenho (PSL). Ele também exibe o número de cargas de trabalho que não

recebem um PSL. Clicar em um gráfico de barras leva você aos workloads em conformidade atribuídos a essa política na página workloads. Clicar no número que segue o gráfico de barras leva você aos workloads em conformidade e não conformes atribuídos a essa política.

## Painel de segurança

O painel Segurança apresenta o status de segurança de alto nível para todos os clusters ou um único cluster, dependendo da exibição atual. Este painel apresenta:

- uma lista dos eventos de segurança recebidos nas últimas 24 horas. Clique em um evento para exibir os detalhes na página de detalhes do evento
- o status de segurança do cluster (contagem de clusters compatíveis e não compatíveis)
- O status de segurança da VM de storage (contagem de VMs de storage em conformidade e não compatíveis)
- o status da criptografia de volume (contagem dos volumes criptografados ou não criptografados)
- o status do volume anti-ransomware (contagem de volumes com anti-ransomware ativados ou desativados)

Você pode clicar nos gráficos de barras dos clusters em conformidade e não compatíveis, VMS de armazenamento, volumes criptografados e não criptografados e status de volume anti-ransomware para acessar as respectivas páginas e exibir os detalhes de segurança dos clusters filtrados, VMs de armazenamento e volumes.

A conformidade baseia-se no "[Guia de endurecimento de segurança da NetApp para ONTAP 9](#)". Clique na seta para a direita na parte superior do painel para exibir os detalhes de segurança de todos os clusters na página Segurança. Para obter informações, "[Visualização do status de segurança detalhado dos clusters e das VMs de storage](#)" consulte .

## Painel de proteção de dados

Esse painel exibe o resumo de proteção de dados de um único ou todos os clusters em um data center. Ele exibe o número total de eventos de proteção de dados, eventos MetroCluster e número de eventos ativos levantados nas últimas 24 horas no ONTAP. Clicar no link de cada um desses eventos leva você à página de detalhes do evento. Você pode clicar no link **Exibir tudo** para exibir todos os eventos de proteção ativa na página de inventário do Gerenciamento de Eventos. O painel exibe:

- Número de volumes em um cluster ou todos os clusters em um data center protegido por cópias Snapshot.
- O número de volumes em um cluster ou todos os clusters em um data center protegido por relacionamentos do SnapMirror. Para relacionamentos SnapMirror, a contagem de volume no cluster de origem é considerada.
- O número de clusters ou todos os clusters em um data center protegido pela configuração MetroCluster por IP ou FC.
- O número de relacionamentos de volume com o atraso do objetivo do ponto de restauração (RPO) do SnapMirror com base no status de atraso.

Você pode passar o Mouse para ver as respectivas contagens e legendas. Você pode clicar na seta para a direita na parte superior do painel para exibir os detalhes de um único ou de todos os clusters na página proteção de dados. Além disso, você pode clicar em:

- Os gráficos de barras de volumes e volumes não protegidos por cópias Snapshot para acessar a página volumes e visualizar os detalhes.

- Os gráficos de barras dos clusters protegidos ou não protegidos pela configuração do MetroCluster para ir para a página clusters e exibir os detalhes.
- Os gráficos de barras para todas as relações vão para a página relacionamentos, onde os detalhes são filtrados com base no cluster de origem.

Para obter mais informações, ["Visualização do estado da proteção do volume"](#) consulte .

### **Painel Visão geral de utilização**

Ao visualizar todos os clusters, você pode optar por exibir clusters classificados por IOPS mais alto, maior taxa de transferência (MB/s) ou maior capacidade física usada.

Ao visualizar um único cluster, você pode optar por exibir cargas de trabalho classificadas por IOPS mais alto, maior taxa de transferência (MB/s) ou maior capacidade lógica usada.

### **Informações relacionadas**

["Correção de problemas usando as correções automáticas do Unified Manager"](#)

["Exibindo informações sobre eventos de desempenho"](#)

["Gerenciamento da performance com a capacidade de performance e as informações de IOPS disponíveis"](#)

["Página de detalhes de volume / Saúde"](#)

["Análise e notificação de eventos de performance"](#)

["Descrição dos tipos de gravidade do evento"](#)

["Fontes de eventos de desempenho"](#)

["Gerenciamento dos objetivos de segurança do cluster"](#)

["Monitoramento do desempenho do cluster na página de destino do cluster de desempenho"](#)

["Monitorando o desempenho usando as páginas Inventário de desempenho"](#)

## **Gerenciamento de recursos ou problemas do ONTAP diretamente do Unified Manager**

Você pode corrigir certos problemas do ONTAP ou gerenciar certos recursos do ONTAP diretamente na interface de usuário do Unified Manager, em vez de usar o Gerenciador de sistema do ONTAP ou a CLI do ONTAP. A opção ["ações de gerenciamento"](#) fornece correções para vários problemas do ONTAP que acionaram eventos do Unified Manager.

Você pode corrigir problemas diretamente na página [ações de gerenciamento](#) selecionando a opção **ações de gerenciamento** no painel de navegação esquerdo. As ações de gerenciamento também estão disponíveis no painel [ações de gerenciamento](#) na página Painel, detalhes do evento e seleção análise de carga de trabalho no menu de navegação à esquerda.

Há certos problemas que o Unified Manager faz o diagnóstico completo e fornece uma única resolução. Para certos recursos do ONTAP, como monitoramento antirransomware, o Unified Manager realiza verificações internas e recomenda ações específicas. Quando disponíveis, essas resoluções são exibidas em ações de gerenciamento com um botão **Fix it**. Clique no botão **Fix it** para corrigir o problema. Tem de ter a função

Administrador de aplicações ou Administrador de armazenamento.

O Unified Manager envia comandos ONTAP ao cluster para fazer a correção solicitada. Quando a correção está concluída, o evento fica obsoleto.

Algumas ações de gerenciamento permitem que você corrija o mesmo problema em vários objetos de armazenamento usando o botão **Fix All**. Por exemplo, pode haver 5 volumes que têm o evento "volume Space Full" que pode ser resolvido clicando na ação de gerenciamento **Fix All** para "Enable volume automático". Um clique permite que você corrija esse problema em volumes 5.

Para obter informações sobre os problemas e recursos do ONTAP que você pode gerenciar usando a correção automática, "[Quais problemas o Unified Manager pode corrigir](#)" consulte .

### Que opções tenho quando vejo o botão corrigir ou corrigir tudo

A página ações de gerenciamento fornece o botão **Fix it** ou **Fix All** para corrigir problemas sobre os quais o Unified Manager foi notificado por meio de um evento.

Recomendamos que você clique nos botões para corrigir um problema, conforme necessário. No entanto, se você não tiver certeza de que deseja resolver o problema conforme recomendado pelo Unified Manager, poderá executar as seguintes ações:

O que você quer fazer?	Ação
Solicite ao Unified Manager que corrija o problema em todos os objetos identificados.	Clique no botão <b>Fix All</b> .
Não corrija o problema de nenhum dos objetos identificados neste momento e oculte essa ação de gerenciamento até que o evento seja levantado novamente.	Clique na seta para baixo e clique em <b>Descartar tudo</b> .
Corrija o problema apenas em alguns dos objetos identificados.	Clique no nome da ação de gerenciamento para expandir a lista e mostrar todas as ações individuais <b>Fix it</b> .em seguida, siga as etapas para corrigir ou descartar ações individuais de gerenciamento.

O que você quer fazer?	Ação
Peça ao Unified Manager para corrigir o problema.	Clique no botão <b>Fix it</b> .
Não corrija o problema neste momento e oculte essa ação de gerenciamento até que o evento seja levantado novamente.	Clique na seta para baixo e clique em <b>Descartar</b> .



O que você quer fazer?	Ação
Exiba os detalhes deste evento para que você possa entender melhor o problema.	<ul style="list-style-type: none"> <li>• Clique no botão <b>Fix it</b> e revise a correção que será aplicada na caixa de diálogo resultante.</li> <li>• Clique na seta para baixo e clique em <b>Exibir detalhes do evento</b> para exibir a página de detalhes do evento.</li> </ul> <p>Em seguida, clique em <b>Fix it</b> de qualquer uma dessas páginas resultantes se você quiser corrigir o problema.</p>
Exiba os detalhes desse objeto de armazenamento para que você possa entender melhor o problema.	Clique no nome do objeto de armazenamento para exibir detalhes na página Performance Explorer ou Health Details.

Em alguns casos, a correção é refletida na próxima sondagem de configuração de 15 minutos. Em outros casos, pode levar até muitas horas para que a alteração de configuração seja verificada e para que o evento seja obsoleto.

Para ver a lista de ações de gerenciamento concluídas ou em andamento, clique no ícone de filtro e selecione **Concluído** ou **em andamento**.

Corrigir todas as operações executadas de forma serial, portanto, quando você visualizar o painel **em andamento** alguns objetos terão o Status **em andamento** enquanto outros terão o Status **agendado**; o que significa que eles ainda estão aguardando para serem implementados.


### Exibindo o status das ações de gerenciamento que você escolheu corrigir

Você pode exibir o status de todas as ações de gerenciamento que você escolheu corrigir na página ações de gerenciamento. A maioria das ações são mostradas como **Completed** bastante rapidamente depois que o Unified Manager envia o comando ONTAP para o cluster. No entanto, algumas ações, como mover um volume, podem levar mais tempo.

Há três filtros disponíveis na página ações de gerenciamento:

- **Completed** mostra as ações de gerenciamento concluídas com êxito e as que falharam. **As ações falhadas** fornecem um motivo para a falha para que você possa resolver o problema manualmente.
- **Em andamento** mostra tanto as ações de gerenciamento que estão sendo implementadas, quanto as que estão programadas para serem implementadas.
- **Recomendado** mostra todas as ações de gerenciamento que estão ativas atualmente para todos os clusters monitorados.

### Passos

1. Clique em **ações de gerenciamento** no painel de navegação esquerdo. Alternativamente, clique  na parte superior do painel **ações de gerenciamento** no painel **Painel** e selecione a exibição que deseja ver.

É apresentada a página ações de gestão.

2. Você pode clicar no ícone de cuidado ao lado da ação de gerenciamento no campo **Description** para ver detalhes sobre o problema e o comando que está sendo usado para corrigir o problema.
3. Para ver quaisquer ações que **falhou**, classifique na coluna **Status** na Exibição **Completed**. Você pode usar a ferramenta **Filter** para essa mesma finalidade.
4. Se você quiser ver mais informações sobre uma ação de gerenciamento de falha ou se decidir que deseja corrigir uma ação de gerenciamento recomendada, clique em **Exibir detalhes do evento** na área expandida depois de clicar no ícone de cuidado ao lado da ação de gerenciamento. Um botão **Fix it** está disponível nessa página.

### Quais problemas o Unified Manager pode corrigir

Usando o recurso de correção automática do Active IQ Unified Manager, você pode optar por resolver certos problemas do ONTAP ou gerenciar certos recursos do ONTAP, como monitoramento anti-ransomware, de forma eficaz por meio do Unified Manager.

Esta tabela descreve esses problemas ou recursos do ONTAP que você pode gerenciar diretamente por meio do botão **Fix it** ou **Fix All** na IU da Web do Unified Manager.

Nome e Descrição do evento	Ação de Gestão	Operação "corrigir"
<p>Volume espaço cheio</p> <p>O volume está quase fora do espaço e violou o limite máximo de capacidade. Este limite é definido por padrão para 90% do tamanho do volume.</p>	Ativar volume com crescimento automático	O Unified Manager determina que o volume com crescimento automático não está configurado para esse volume, portanto, habilita esse recurso para que o volume aumente na capacidade quando necessário.
<p>Inodes Full</p> <p>Este volume ficou sem inodes e não pode aceitar novos arquivos.</p>	Aumentar o número de inodes no volume	Aumenta o número de inodes no volume em 2%.
<p>Detectada não correspondência incorreta da política de nível de armazenamento</p> <p>O volume tem muitos dados inativos e a política de disposição em camadas atual é definida como "somente snapshot" ou "nenhum".</p>	Habilitar a disposição automática de nuvem em categorias	Como o volume já reside em um FabricPool, ele muda a política de disposição em categorias para "automático", para que os dados inativos sejam movidos para a camada de nuvem de menor custo.
<p>Detectada incompatibilidade de nível de armazenamento</p> <p>O volume tem muitos dados inativos, mas não reside em uma categoria de storage habilitado para nuvem (FabricPool).</p>	Alterar a camada de storage dos volumes	Move o volume para a camada de storage habilitada para a nuvem e define a política de disposição em camadas como "automática" para mover dados inativos para a camada de nuvem.

<b>Nome e Descrição do evento</b>	<b>Ação de Gestão</b>	<b>Operação "corrigir"</b>
<p>Registo de auditoria desativado</p> <p>O log de auditoria não está habilitado para a VM de armazenamento</p>	<p>Ativar o registo de auditoria para a VM de armazenamento</p>	<p>Permite o log de auditoria na VM de storage.</p> <p>Observe que a VM de storage já deve ter um local de log de auditoria local ou remoto configurado.</p>
<p>Banner de login desativado</p> <p>O banner de login do cluster deve estar habilitado para aumentar a segurança, deixando as restrições de acesso claras.</p>	<p>Defina o banner de login para o cluster</p>	<p>Define o banner de login do cluster como ""Acesso restrito a usuários autorizados"".</p>
<p>Banner de login desativado</p> <p>O banner de login para a VM de armazenamento deve ser habilitado para aumentar a segurança, deixando as restrições de acesso claras.</p>	<p>Defina o banner de login para a VM de armazenamento</p>	<p>Define o banner de login da VM de armazenamento como "Acesso restrito a usuários autorizados".</p>
<p>O SSH está usando Ciphers inseguros</p> <p>Cifras com o sufixo "-cbc" são consideradas inseguras.</p>	<p>Remova cifras inseguras do cluster</p>	<p>Remove as cifras inseguras — como aes192-cbc e AES128-cbc — do cluster.</p>
<p>O SSH está usando Ciphers inseguros</p> <p>Cifras com o sufixo "-cbc" são consideradas inseguras.</p>	<p>Remova cifras inseguras da VM de armazenamento</p>	<p>Remove as cifras inseguras - como aes192-cbc e AES128-cbc — da VM de storage.</p>
<p>Transporte HTTPS AutoSupport desativado</p> <p>O protocolo de transporte utilizado para enviar mensagens AutoSupport para o suporte técnico deve ser encriptado.</p>	<p>Defina HTTPS como o protocolo de transporte para mensagens AutoSupport</p>	<p>Define HTTPS como o protocolo de transporte de mensagens AutoSupport no cluster.</p>

Nome e Descrição do evento	Ação de Gestão	Operação "corrigir"
<p>Limite de desequilíbrio de carga do cluster violado</p> <p>Indica que a carga está desequilibrada entre os nós no cluster. Esse evento é gerado quando a variação da capacidade de performance usada é superior a 30% entre nós.</p>	Equilibre workloads de cluster	O Unified Manager identifica o melhor volume para mover de um nó para o outro, a fim de reduzir o desequilíbrio e, em seguida, move o volume.
<p>Limite de desequilíbrio da capacidade do cluster violado</p> <p>Indica que a capacidade está desequilibrada entre os agregados no cluster. Este evento é gerado quando a variação da capacidade utilizada é superior a 70% entre agregados.</p>	Equilibrar a capacidade do cluster	O Unified Manager identifica o melhor volume para mover de um agregado para outro, a fim de reduzir o desequilíbrio e, em seguida, move o volume.
<p>Limite de capacidade de performance usado violado</p> <p>Indica que a carga no nó pode se tornar sobreutilizada se você não reduzir a utilização de uma ou mais cargas de trabalho altamente ativas. Esse evento é gerado quando o valor da capacidade de performance do nó usada for superior a 100% por mais de 12 horas.</p>	Limite a carga alta no nó	O Unified Manager identifica o volume com o IOPS mais alto e aplica uma política de QoS usando os níveis histórico esperado e máximo de IOPS para reduzir a carga no nó.
<p>Limite de aviso de eventos dinâmicos violado</p> <p>Indica que o nó já está operando em um estado sobrecarregado devido à carga anormalmente alta de algumas das cargas de trabalho.</p>	Reduza a sobrecarga no nó	O Unified Manager identifica o volume com o IOPS mais alto e aplica uma política de QoS usando os níveis histórico esperado e máximo de IOPS para reduzir a carga no nó.
<p>A aquisição não é possível</p> <p>O failover está atualmente desativado, portanto, o acesso aos recursos do nó durante uma interrupção ou reinicialização seria perdido até que o nó ficasse disponível novamente.</p>	Habilite o failover de nó	O Unified Manager envia o comando apropriado para habilitar o failover em todos os nós do cluster.

Nome e Descrição do evento	Ação de Gestão	Operação "corrigir"
<p>A opção Cf.Takeover.ON_PANIC está configurada como DESLIGADA</p> <p>A opção nodeshell "cf.Takeover.on_panic" está definida como <b>Off</b>, o que pode causar um problema em sistemas configurados pelo HA.</p>	<p>Ativar a aquisição em pânico</p>	<p>O Unified Manager envia o comando apropriado ao cluster para alterar essa configuração para <b>ON</b>.</p>
<p>Desative a opção nodeshell SnapMirror.enable</p> <p>A antiga opção nodeshell "SnapMirror.enable" está definida como <b>ON</b>, o que pode causar um problema durante a inicialização após a atualização para o ONTAP 9.3 ou superior.</p>	<p>Defina a opção SnapMirror.enable (Ativar) como Off (Desligado)</p>	<p>O Unified Manager envia o comando apropriado ao cluster para alterar essa configuração para <b>Off</b>.</p>
<p>Telnet ativado</p> <p>Indica um potencial problema de segurança porque o Telnet é inseguro e passa dados de maneira não criptografada.</p>	<p>Desativar o Telnet</p>	<p>O Unified Manager envia o comando apropriado ao cluster para desativar o Telnet.</p>
<p>Configurar a aprendizagem anti-ransomware de VM de storage</p> <p>Verifica periodicamente clusters com licenças para monitoramento anti-ransomware. Valida se uma VM de armazenamento suporta apenas volumes NFS ou SMB em um cluster desse tipo.</p>	<p>Colocar as VMs de storage em um <i>learning</i> modo de monitoramento anti-ransomware</p>	<p>O Unified Manager define o monitoramento anti-ransomware para <i>learning</i> indicar as VMs de storage por meio do console de gerenciamento de cluster. O monitoramento contra ransomware em todos os novos volumes criados na VM de storage é automaticamente movido para o modo de aprendizado. Com essa capacitação, o ONTAP pode aprender o padrão de atividade nos volumes e detectar anomalias devido a possíveis ataques mal-intencionados.</p>

Nome e Descrição do evento	Ação de Gestão	Operação "corrigir"
<p>Configurar o volume de aprendizagem anti-ransomware</p> <p>Verifica periodicamente clusters com licenças para monitoramento anti-ransomware. Valida se um volume suporta apenas serviços NFS ou SMB em tal cluster.</p>	<p>Coloque volumes <code>learning</code> no modo de monitoramento anti-ransomware</p>	<p>O Unified Manager define o monitoramento anti-ransomware para <code>learning</code> indicar os volumes pelo console de gerenciamento de cluster. Com essa capacitação, o ONTAP pode aprender o padrão de atividade nos volumes e detectar anomalias devido a possíveis ataques mal-intencionados.</p>
<p>Habilite o volume anti-ransomware</p> <p>Verifica periodicamente clusters com licenças para monitoramento anti-ransomware. Detecta se os volumes estão <code>learning</code> no modo de monitoramento anti-ransomware por mais de 45 dias e determina a perspectiva de colocá-los no modo ativo.</p>	<p>Coloque volumes <code>active</code> no modo de monitoramento anti-ransomware</p>	<p>O Unified Manager define o monitoramento anti-ransomware para <code>active</code> os volumes por meio do console de gerenciamento de cluster. Com essa capacitação, o ONTAP pode aprender o padrão de atividade nos volumes, detectar anomalias devido a possíveis ataques maliciosos e criar alertas de ações de proteção de dados.</p>
<p>Desativar volume anti-ransomware</p> <p>Verifica periodicamente clusters com licenças para monitoramento anti-ransomware. Detecta notificações repetitivas durante o monitoramento ativo anti-ransomware nos volumes (por exemplo, vários avisos de possíveis ataques de ransomware são retornados ao longo de 30 dias).</p>	<p>Desativar o monitoramento anti-ransomware em volumes</p>	<p>O Unified Manager desativa o monitoramento anti-ransomware nos volumes por meio do console de gerenciamento de cluster.</p>

### Substituindo ações de gerenciamento por meio de scripts

Você pode criar scripts personalizados e associá-los a alertas para realizar ações específicas para eventos específicos e não optar pelas ações de gerenciamento padrão disponíveis para eles na página ações de gerenciamento ou no painel do Unified Manager.

Se você quiser executar ações específicas para um tipo de evento e optar por não corrigi-las como parte da capacidade de ação de gerenciamento fornecida pelo Unified Manager, você pode configurar um script personalizado para a ação específica. Em seguida, você pode associar o script a um alerta para esse tipo de evento e cuidar de tais eventos individualmente. Nesse caso, as ações de gerenciamento não são geradas para esse tipo de evento específico na página ações de gerenciamento ou no painel do Unified Manager.

## Gerenciamento de clusters

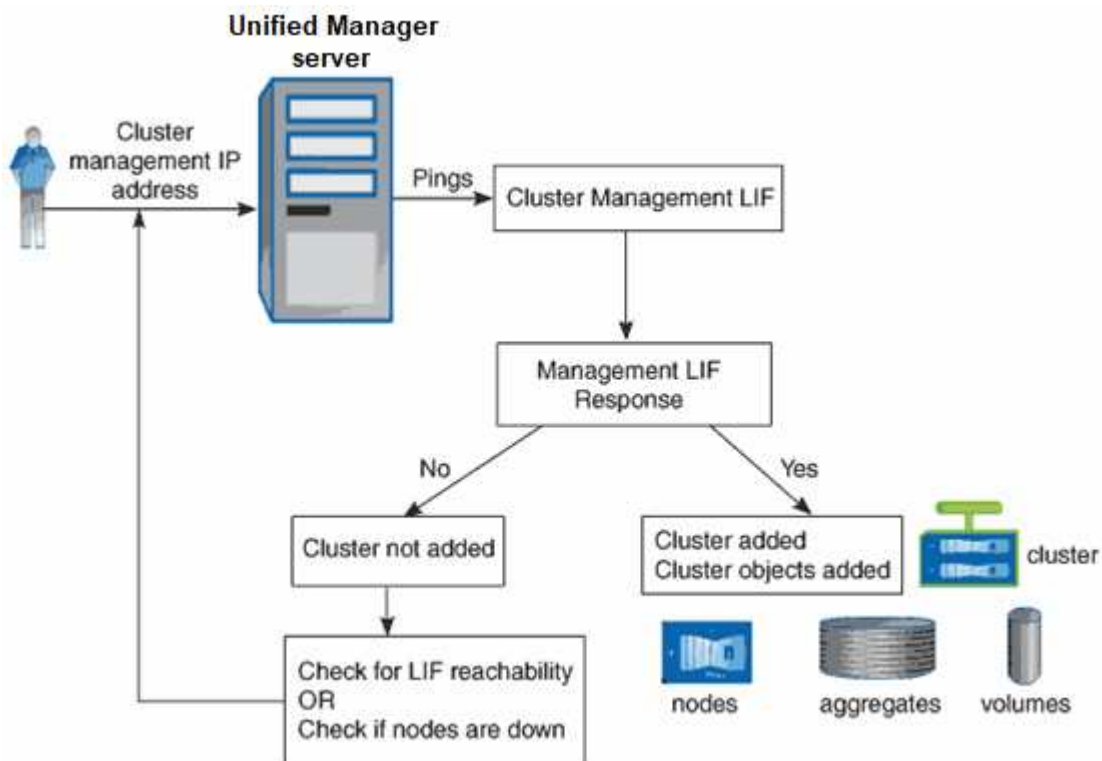
É possível gerenciar os clusters do ONTAP usando o Unified Manager para monitorar, adicionar, editar e remover clusters.

### Como funciona o processo de descoberta de cluster

Depois de adicionar um cluster ao Unified Manager, o servidor descobre os objetos do cluster e os adiciona ao banco de dados. Entender como funciona o processo de descoberta ajuda você a gerenciar os clusters da sua organização e seus objetos.

O intervalo de monitorização para a recolha de informações de configuração do cluster é de 15 minutos. Por exemplo, depois de adicionar um cluster, leva 15 minutos para exibir os objetos de cluster na IU do Unified Manager. Esse período de tempo também é verdadeiro ao fazer alterações em um cluster. Por exemplo, se você adicionar dois novos volumes a um SVM em um cluster, verá esses novos objetos na IU após o próximo intervalo de polling, que pode ser de até 15 minutos.

A imagem a seguir ilustra o processo de descoberta:



Depois que todos os objetos de um novo cluster forem descobertos, o Unified Manager começará a coletar dados históricos de desempenho dos 15 dias anteriores. Essas estatísticas são coletadas usando a funcionalidade de coleta de continuidade de dados. Esse recurso fornece mais de duas semanas de informações de desempenho para um cluster imediatamente após ser adicionado. Após a conclusão do ciclo de coleta de continuidade de dados, os dados de desempenho do cluster em tempo real são coletados, por padrão, a cada cinco minutos.



Como a coleta de dados de desempenho de 15 dias é intensiva em CPU, sugere-se que você alterne a adição de novos clusters para que as pesquisas de coleta de continuidade de dados não sejam executadas em muitos clusters ao mesmo tempo.

## Visualização da lista de clusters monitorados

Você pode usar a página Configuração de cluster para exibir seu inventário de clusters. Você pode exibir detalhes sobre os clusters, como nome ou endereço IP e status de comunicação.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

### Passo

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração do cluster**.

Todos os clusters no ambiente de storage gerenciado pelo Unified Manager são exibidos. A lista de clusters é classificada pela coluna nível de gravidade do estado de coleta. Você pode clicar em um cabeçalho de coluna para classificar os clusters por diferentes colunas.

## Adição de clusters

Você pode adicionar um cluster ao Active IQ Unified Manager para que você possa monitorar o cluster. Isso inclui a capacidade de obter informações de cluster, como integridade, capacidade, desempenho e configuração do cluster, para que você possa encontrar e resolver quaisquer problemas que possam ocorrer.

### Antes de começar

- Você deve ter a função Administrador do aplicativo ou a função Administrador do armazenamento.
- Você deve ter as seguintes informações:
  - O Unified Manager dá suporte a clusters ONTAP on-premises, ONTAP Select, Cloud Volumes ONTAP.
  - Você deve ter o nome do host ou o endereço IP de gerenciamento de cluster (IPv4 ou IPv6) para o cluster.

Ao usar o nome do host, ele deve ser resolvido para o endereço IP de gerenciamento de cluster para o LIF de gerenciamento de cluster. Se você usar um LIF de gerenciamento de nós, a operação falhará.

- Tem de ter o nome de utilizador e a palavra-passe para aceder ao cluster.

Essa conta deve ter a função *admin* com acesso ao aplicativo definido como *ontapi*, *console* e *http*.

- Você deve saber o número da porta para se conectar ao cluster usando o protocolo HTTPS (normalmente a porta 443).
- O cluster deve estar executando o software ONTAP versão 9,1 ou superior.
- Você precisa ter espaço adequado no servidor do Unified Manager. Você é impedido de adicionar um cluster ao servidor quando mais de 90% de espaço já estiver consumido.



- Você tem os certificados necessários:

**Certificado SSL (HTTPS):** Este certificado pertence ao Unified Manager. Um certificado SSL (HTTPS) autoassinado padrão é gerado com uma nova instalação do Unified Manager. A NetApp recomenda que você o atualize para um certificado assinado pela CA para obter uma melhor segurança. Se o certificado do servidor expirar, você deverá regenerá-lo e reiniciar o Unified Manager para que os serviços incorporem o novo certificado. Para obter mais informações sobre como regenerar o certificado SSL, "[Gerando um certificado de segurança HTTPS](#)" consulte .

**Certificado EMS:** Este certificado é de propriedade do Unified Manager. Ele é usado durante a autenticação para notificações EMS recebidas do ONTAP.

**Certificados para comunicação TLS mútua:** Usados durante a comunicação TLS mútua entre o Unified Manager e o ONTAP. A autenticação baseada em certificado é ativada para um cluster, com base na versão do ONTAP. Se o cluster que executa a versão do ONTAP for inferior à 9,5, a autenticação baseada em certificado não está ativada.

A autenticação baseada em certificado não será ativada automaticamente para um cluster, se você estiver atualizando uma versão mais antiga do Unified Manager. No entanto, você pode ativá-lo modificando e salvando os detalhes do cluster. Se o certificado expirar, você deve regenerá-lo para incorporar o novo certificado. Para obter mais informações sobre como visualizar e regenerar o certificado, "[Edição de clusters](#)" consulte .



- Você pode adicionar um cluster a partir da IU da Web e a autenticação baseada em certificado é ativada automaticamente.
- Você pode adicionar um cluster por meio da CLI do Unified Manager, a autenticação baseada em certificado não está habilitada por padrão. Se você adicionar um cluster usando a CLI do Unified Manager, será necessário editar o cluster usando a IU do Unified Manager. Você pode ver "[Comandos de CLI do Unified Manager compatíveis](#)" para adicionar um cluster usando a CLI do Unified Manager.
- Se a autenticação baseada em certificado estiver ativada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurar para outro servidor do Unified Manager onde o nome de host ou o endereço IP forem alterados, o monitoramento do cluster poderá falhar. Para evitar a falha, edite e salve os detalhes do cluster. Para obter mais informações sobre como editar os detalhes do cluster, "[Edição de clusters](#)" consulte .
- No nível do cluster, a interface Active IQ adiciona duas novas entradas de grupo de usuários para o método de autenticação "cert".

+

**Certificados de cluster:** Este certificado é de propriedade da ONTAP. Não é possível adicionar um cluster ao Unified Manager com um certificado expirado e, se o certificado já tiver expirado, você deve regenerá-lo antes de adicionar o cluster. Para obter informações sobre a geração de certificados, consulte o artigo da base de conhecimento (KB) "[Como renovar um certificado auto-assinado do ONTAP na interface do utilizador do System Manager](#)" .

- Uma única instância do Unified Manager pode dar suporte a um número específico de nós. Se você precisar monitorar um ambiente que exceda a contagem de nós com suporte, instale uma instância adicional do Unified Manager para monitorar alguns dos clusters. Para exibir a lista de contagem de nós suportados, consulte "[Guia de práticas recomendadas do Unified Manager](#)".

## Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração do cluster**.
2. Na página Configuração de cluster, clique em **Add**.
3. Na caixa de diálogo Adicionar cluster, especifique os valores conforme necessário e clique em **Enviar**.
4. Na caixa de diálogo autorizar host, clique em **Exibir certificado** para exibir as informações do certificado sobre o cluster.
5. Clique em **Sim**.

Depois de salvar os detalhes do cluster, você pode ver o certificado de comunicação TLS mútua para um cluster.

Se a autenticação baseada em certificado não estiver ativada, o Unified Manager verificará o certificado somente quando o cluster for adicionado inicialmente. O Unified Manager não verifica o certificado de cada chamada de API para o ONTAP.

Depois que todos os objetos de um novo cluster forem descobertos, o Unified Manager começará a coletar dados históricos de desempenho dos 15 dias anteriores. Essas estatísticas são coletadas usando a funcionalidade de coleta de continuidade de dados. Esse recurso fornece mais de duas semanas de informações de desempenho para um cluster imediatamente após ser adicionado. Após a conclusão do ciclo de coleta de continuidade de dados, os dados de desempenho do cluster em tempo real são coletados, por padrão, a cada cinco minutos.



Como a coleta de dados de desempenho de 15 dias é intensiva em CPU, sugere-se que você alterne a adição de novos clusters para que as pesquisas de coleta de continuidade de dados não sejam executadas em muitos clusters ao mesmo tempo. Além disso, se você reiniciar o Unified Manager durante o período de coleta de continuidade de dados, a coleta será interrompida e você verá lacunas nos gráficos de desempenho para o período de tempo em falta.

Se receber uma mensagem de erro que não pode adicionar o cluster, verifique se existem os seguintes problemas:



- Se os relógios nos dois sistemas não estiverem sincronizados e a data de início do certificado HTTPS do Unified Manager for posterior à data no cluster. Você deve garantir que os relógios são sincronizados usando NTP ou um serviço similar.
- Se o cluster tiver atingido o número máximo de destinos de notificação EMS, o endereço do Unified Manager não poderá ser adicionado. Por predefinição, apenas podem ser definidos 20 destinos de notificação EMS no cluster.

## Informações relacionadas

["Adicionando usuários"](#)

["Visualizar a lista de cluster e os detalhes"](#)

["Instalando um certificado HTTPS assinado e retornado pela CA"](#)

## Edição de clusters

Você pode modificar as configurações de um cluster existente, como nome do host ou

endereço IP, nome de usuário, senha e porta, usando a caixa de diálogo Editar cluster.

### Antes de começar

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



A partir do Unified Manager 9,7, os clusters podem ser adicionados apenas usando HTTPS.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração do cluster**.
2. Na página **Configuração de cluster**, selecione o cluster que deseja editar e clique em **Editar**.
3. Na caixa de diálogo **Editar Cluster**, modifique os valores conforme necessário. Se você tiver modificado os detalhes de um cluster adicionado ao Unified Manager, poderá exibir os detalhes do certificado para comunicação TLS mútua, com base na versão do ONTAP. Para obter mais informações sobre a versão do ONTAP, "[Certificados para comunicação TLS mútua](#)" consulte . Você pode ver os detalhes do certificado clicando em **Detalhes do certificado**. Se o certificado tiver expirado, clique no botão **regenerar** para incorporar o novo certificado.
4. Clique em **Enviar**.
5. Na caixa de diálogo autorizar host, clique em **Exibir certificado** para exibir as informações do certificado sobre o cluster.
6. Clique em **Sim**.

### Informações relacionadas

["Adicionando usuários"](#)

["Visualizar a lista de cluster e os detalhes"](#)

## Remoção de clusters

Você pode remover um cluster do Unified Manager usando a página Configuração de cluster. Por exemplo, você pode remover um cluster se a descoberta de cluster falhar ou quando quiser desativar um sistema de storage.

### Antes de começar

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

Esta tarefa remove o cluster selecionado do Unified Manager. Depois que um cluster é removido, ele não é mais monitorado. A instância do Unified Manager registrada com o cluster removido também não é registrada do cluster.

A remoção de um cluster também exclui todos os objetos de armazenamento, dados históricos, serviços de armazenamento e todos os eventos associados do Unified Manager. Essas alterações são refletidas nas páginas de inventário e nas páginas de detalhes após o próximo ciclo de coleta de dados.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração do cluster**.
2. Na página Configuração do cluster, selecione o cluster que deseja remover e clique em **Remover**.

3. Na caixa de diálogo **Remover fonte de dados**, clique em **Remover** para confirmar a solicitação de remoção.

#### Informações relacionadas

["Adicionando usuários"](#)

["Visualizar a lista de cluster e os detalhes"](#)

## Redescobrir clusters

É possível redescobrir manualmente um cluster a partir da página Configuração do cluster para obter as informações mais recentes sobre a integridade, o status do monitoramento e o status do desempenho do cluster.

Você pode redescobrir manualmente um cluster quando quiser atualizar o cluster, como aumentando o tamanho de um agregado quando houver espaço insuficiente, e deseja que o Unified Manager descubra as alterações feitas.

Quando o Unified Manager é emparelhado com o OnCommand Workflow Automation (WFA), o emparelhamento aciona a reaquisição dos dados armazenados em cache pelo WFA.

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração do cluster**.
2. Na página **Configuração de cluster**, clique em **redescobrir**.

O Unified Manager redescobre o cluster selecionado e exibe o status de integridade e desempenho mais recente.

#### Informações relacionadas

["Visualizar a lista de cluster e os detalhes"](#)

## Monitoramento da infraestrutura virtual VMware

O Active IQ Unified Manager oferece visibilidade das máquinas virtuais (VMs) em sua infraestrutura virtual e permite monitorar e solucionar problemas de storage e performance em seu ambiente virtual. Você pode usar esse recurso para determinar quaisquer problemas de latência no ambiente de storage ou quando houver um evento de desempenho relatado no vCenter Server.

Uma implantação típica de infraestrutura virtual no ONTAP tem vários componentes espalhados pelas camadas de computação, rede e storage. Qualquer atraso de desempenho em uma aplicação de VM pode ocorrer devido a uma combinação de latências enfrentadas pelos vários componentes nas respectivas camadas. Esse recurso é útil para administradores de storage e do vCenter Server e GENERALISTAS DE TI que precisam analisar um problema de desempenho em um ambiente virtual e entender em qual componente o problema ocorreu.

Agora você pode acessar o vCenter Server no menu do vCenter da seção VMware. A visualização de cada máquina virtual listada tem o link **VCENTER Server** na VISUALIZAÇÃO DE TOPOLOGIA que inicia o vCenter

Server em um novo navegador. Você também pode usar o botão **expandir topologia** para iniciar o vCenter Server e clicar no botão **Exibir no vCenter** para exibir os datastores no vCenter Server.

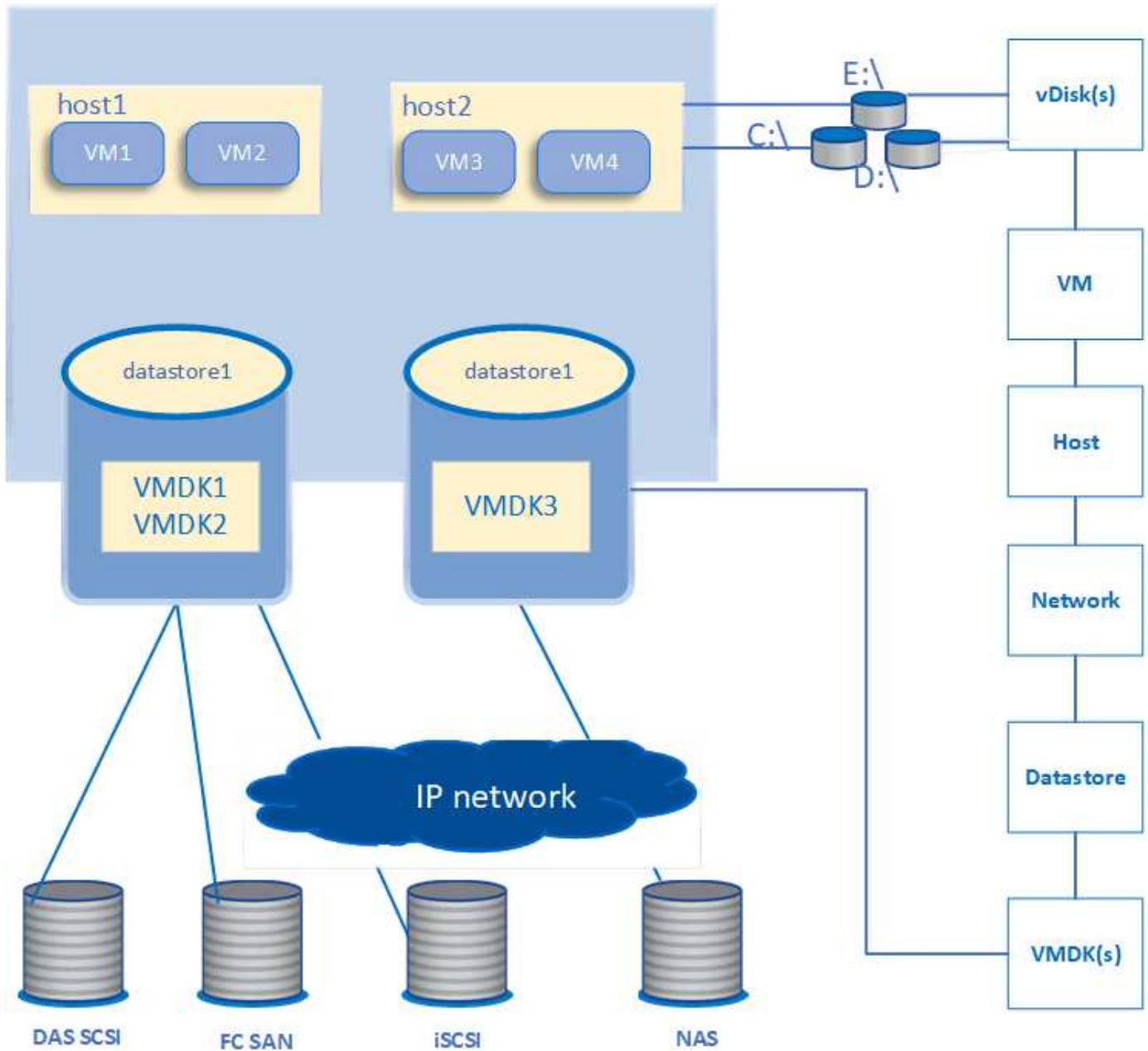
O Unified Manager apresenta o subsistema subjacente de um ambiente virtual em uma visualização topológica para determinar se ocorreu um problema de latência no nó de computação, na rede ou no storage. A visualização também destaca o objeto específico que causa o atraso de desempenho para tomar medidas corretivas e solucionar o problema subjacente.

Uma infraestrutura virtual implantada no storage ONTAP inclui os seguintes objetos:

- VCenter Server: Um plano de controle centralizado para gerenciar as VMs VMware, os hosts ESXi e todos os componentes relacionados em um ambiente virtual. Para obter mais informações sobre o vCenter Server, consulte a documentação da VMware.
- Host: Um sistema físico ou virtual que executa o ESXi, o software de virtualização da VMware e hospeda a VM.
- Datastore: Datastores são objetos de armazenamento virtual conectados aos hosts ESXi. Armazenamentos de dados são entidades de storage gerenciáveis do ONTAP, como LUNs ou volumes, usadas como um repositório para arquivos de VM, como arquivos de log, scripts, arquivos de configuração e discos virtuais. Eles são conectados aos hosts no ambiente por meio de uma conexão de rede SAN ou IP. Armazenamentos de dados fora do ONTAP que são mapeados para o vCenter Server não são suportados nem exibidos no Unified Manager.
- VM: Uma máquina virtual VMware.
- Discos virtuais: Os discos virtuais em datastores pertencentes às VMs que têm uma extensão como VMDK. Os dados de um disco virtual são armazenados no VMDK correspondente.
- VMDK: Um disco de máquina virtual no datastore que fornece espaço de armazenamento para discos virtuais. Para cada disco virtual, há um VMDK correspondente.

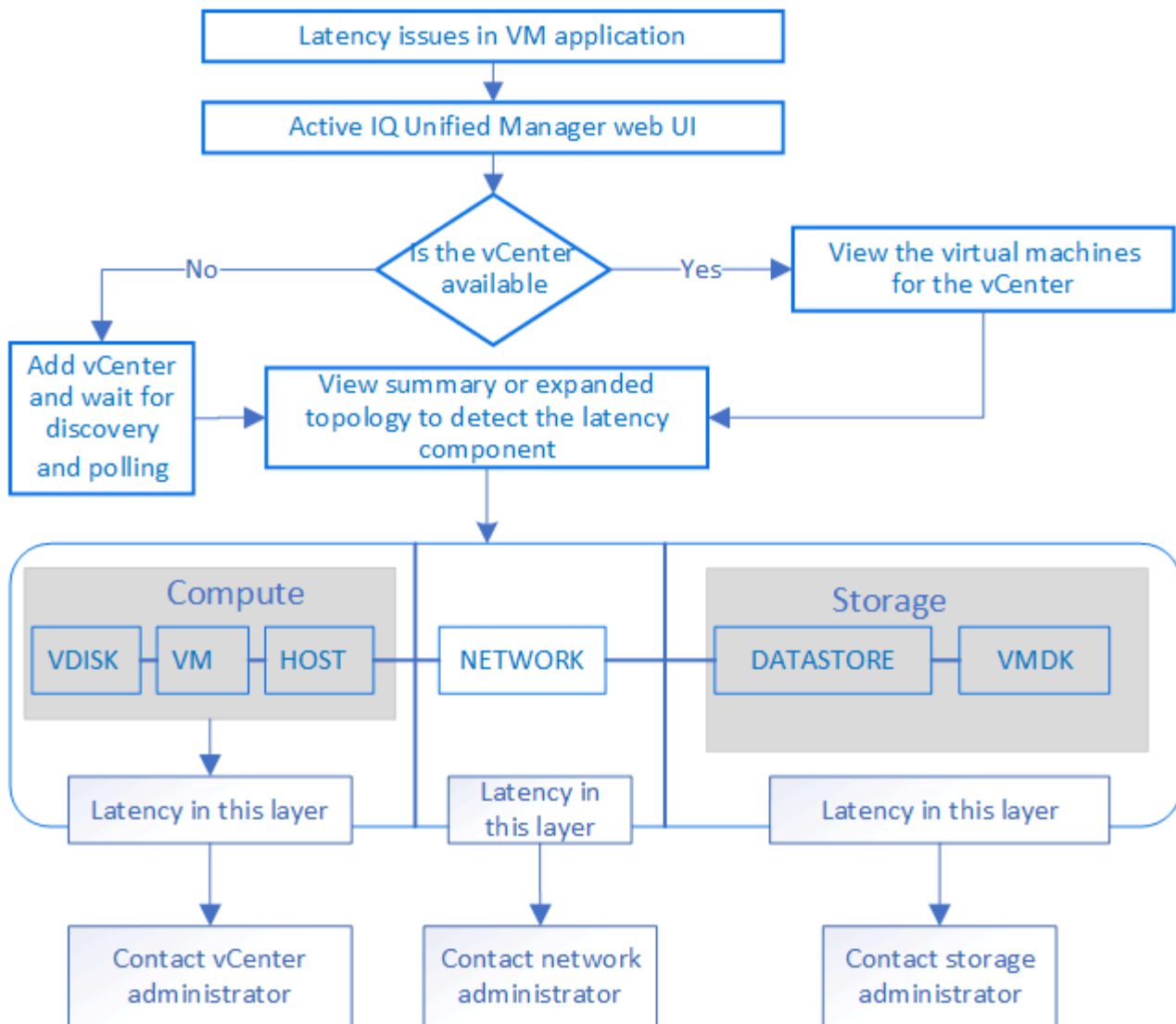
Esses objetos são representados em uma visualização de topologia de VM.

## **Virtualização VMware no ONTAP**



### Fluxo de trabalho do usuário

O diagrama a seguir exibe um caso de uso típico do uso da exibição de topologia da VM:



## O que não é suportado

- Armazenamentos de dados que estão fora do ONTAP e são mapeados para as instâncias do vCenter Server não são suportados no Unified Manager. Quaisquer VMs com discos virtuais nesses datastores também não são suportadas.
- Um datastore que se estende por vários LUNs não é suportado.
- Armazenamentos de dados usando conversão de endereços de rede (NAT) para mapeamento de dados LIF (ponto de extremidade de acesso) não são suportados.
- A exportação de volumes ou LUNs como datastores em clusters diferentes com os mesmos endereços IP em uma configuração de vários LIFs não é suportada, pois o Unified Manager não consegue identificar qual datastore pertence a qual cluster.

Exemplo: Suponha que o cluster A tenha datastore A. datastore A é exportado via data LIF com o mesmo endereço IP x.x.x.x e a VM A é criada neste datastore. Da mesma forma, o cluster B tem datastore B. o datastore B é exportado via data LIF com o mesmo endereço IP x.x.x.x e a VM B é criada no datastore B. O UM não será capaz de mapear o datastore A para a topologia da VM A para o volume/LUN ONTAP correspondente nem mapear a VM B.

- Somente os volumes nas e SAN (iSCSI e FCP para VMFS) são compatíveis como armazenamentos de dados, os volumes virtuais (vVols) não são compatíveis.

- Apenas são suportados discos virtuais iSCSI. Discos virtuais dos tipos NVMe e SATA não são suportados.
- As vistas não permitem gerar relatórios para analisar o desempenho dos vários componentes.
- Para a configuração de recuperação de desastres (DR) de máquina virtual de armazenamento (VM de armazenamento) compatível apenas com a infraestrutura virtual no Unified Manager, a configuração deve ser alterada manualmente no vCenter Server para apontar para os LUNs ativos em cenários de comutação e switchback. Sem uma intervenção manual, seus datastores ficam inacessíveis.

## Visualização e adição do vCenter Server

Para visualizar e solucionar problemas de desempenho das máquinas virtuais (VMs), os vCenter Servers associados devem ser adicionados à sua instância do Active IQ Unified Manager.

### Antes de começar

Antes de adicionar ou visualizar o vCenter Servers, verifique o seguinte:

- Você está ciente dos nomes do vCenter Server.
- Você conhece o endereço IP do vCenter Server e tem as credenciais necessárias. As credenciais devem ser de um administrador do vCenter Server ou de um usuário raiz com acesso somente leitura ao vCenter Server.
- O vCenter Server que você deseja adicionar executa o vSphere 6,5 ou posterior.



O suporte do Unified Manager para VMware ESXi e vCenter Server está disponível em inglês e japonês.

- A configuração de coleta de dados no vCenter Server é definida como o nível de estatísticas *Level 3* do , garantindo o nível necessário de coleta de métricas para todos os objetos monitorados. A duração do intervalo deve ser *5 minutes*, e o período de gravação deve ser *1 day*.

Para obter mais informações, consulte a seção "níveis de coleta de dados" do *Guia de monitoramento e desempenho do vSphere* na documentação da VMware.

- Os valores de latência no vCenter Server são configurados em milissegundos, e não em microssegundos, para cálculos bem-sucedidos dos valores de latência.
- Ao adicionar o datastore ao vCenter Server, você pode usar o endereço IP do host ou o nome de domínio totalmente qualificado (FQDN). Caso você esteja adicionando FQDN, verifique se o nome de domínio pode ser resolvido pelo servidor do Unified Manager. Por exemplo, para uma instalação Linux, certifique-se de que o nome de domínio é adicionado `/etc/resolv.conf` no arquivo.
- A hora atual do vCenter Server está em sincronia com o fuso horário do vCenter Server.
- O vCenter Server está acessível para uma descoberta bem-sucedida.
- Você tem acesso de leitura ao VMware SDK ao adicionar o vCenter Server ao Unified Manager. Isso é necessário para a polling de configuração.

Para cada vCenter Server adicionado e descoberto, o Unified Manager coleta os dados de configuração, como detalhes do vCenter Server e do servidor ESXi, mapeamento do ONTAP, detalhes do datastore e número de VMs hospedadas. Ele coleta ainda mais as métricas de desempenho dos componentes.

### Passos

1. Vá para **VMware > vCenter** e verifique se o vCenter Server está disponível na lista.





Se o vCenter Server não estiver disponível, você deverá adicionar o vCenter Server.

- a. Clique em **Add**.
- b. Adicione o endereço IP correto para o vCenter Server e verifique se o dispositivo está acessível.
- c. Adicione o nome de usuário e a senha do administrador ou usuário raiz com acesso somente leitura ao vCenter Server.
- d. Adicione o número de porta personalizado se estiver usando qualquer porta diferente da 443 padrão.
- e. Clique em **Salvar**.

Após a descoberta bem-sucedida, um certificado de servidor é exibido para você aceitar.

Quando você aceita o certificado, o vCenter Server é adicionado à lista de vCenter Servers disponíveis. A adição do dispositivo não resulta na coleta de dados para as VMs associadas, e a coleta ocorre nos intervalos programados.

2. Se o vCenter Server estiver disponível na página **vCenters**, verifique seu status passando o Mouse sobre o campo **Status** para exibir se o vCenter Server está funcionando conforme esperado ou se há um aviso ou erro.



A adição do vCenter Server permite exibir os seguintes status. No entanto, os dados de desempenho e latência das VMs correspondentes podem levar até uma hora depois de adicionar o vCenter Server para serem refletidos com precisão.

- Verde: "Normal", indicando que o vCenter Server foi descoberto e as métricas de desempenho foram coletadas com sucesso
  - Amarelo: "Aviso" (por exemplo, quando o nível de estatísticas do vCenter Server não foi definido como 3 ou superior para obter estatísticas para cada objeto)
  - Laranja: "Erro" (indica quaisquer erros internos, como exceção, falha na coleta de dados de configuração ou o vCenter Server não está acessível) você pode clicar no ícone de exibição de coluna (**Mostrar/Ocultar**) para exibir a mensagem de status de um status do vCenter Server e solucionar o problema.
3. Caso o vCenter Server esteja inacessível ou as credenciais tenham sido alteradas, edite os detalhes do vCenter Server selecionando **vCenter > Editar**.
  4. Faça as alterações necessárias na página **Editar VMware vCenter Server**.
  5. Clique em **Salvar**.

### A coleta de dados do vCenter Server começa

O vCenter Server coleta amostras de dados de desempenho em tempo real de 20 segundos e as acumula até 5 minutos de amostras. A programação para coleta de dados de desempenho do Unified Manager é baseada nas configurações padrão do vCenter Server. O Unified Manager processa as amostras de 5 minutos obtidas do vCenter Server e calcula uma média horária do IOPS e da latência dos discos virtuais, VMs e hosts. Para datastores, o Unified Manager calcula uma média horária do IOPS e da latência de amostras obtidas do ONTAP. Estes valores estão disponíveis no topo da hora. As métricas de desempenho não estão disponíveis imediatamente após a adição do vCenter Server e estão disponíveis somente quando a próxima hora for iniciada. A pesquisa de dados de desempenho começa ao concluir um ciclo de coleta de dados de configuração.

Para consultar dados de configuração do vCenter Server, o Unified Manager segue o mesmo cronograma de coleta de dados de configuração do cluster. Para obter informações sobre a configuração do vCenter Server e

o agendamento de coleta de dados de desempenho, consulte "Configuração de cluster e atividade de coleta de dados de desempenho".

## Informações relacionadas

["Atividade de coleta de dados de desempenho e configuração de cluster"](#)

## Remoção do vCenter Server

Você pode remover o vCenter Servers da sua instância do Active IQ Unified Manager. Por exemplo, você pode remover um vCenter Server se a descoberta do vCenter Server falhar ou quando ela não for mais necessária.

A remoção de um vCenter Server também exclui todas as máquinas virtuais (VMs) hospedadas nesse vCenter e seus dados de configuração. Depois que o vCenter Server for removido, ele não será mais monitorado, juntamente com seus objetos associados e dados históricos. Essas alterações serão refletidas nas páginas de inventário do vCenter e da máquina virtual.

### Antes de começar

Antes de remover o vCenter Servers, verifique o seguinte:

- Você tem a função Administrador de aplicativos ou a função Administrador de armazenamento.
- Você deve estar ciente dos nomes do vCenter Server e respectivos endereços IP associados a eles.

### Passos

1. No painel de navegação à esquerda, clique em **VMware>vCenter**.
2. Na página vCenters, selecione o vCenter Server que deseja remover e clique em **Remover**.
3. Na caixa de diálogo **Remover vCenter**, clique em **OK** para confirmar a solicitação de remoção.

## Monitoramento de máquinas virtuais

Para qualquer problema de latência nas aplicações de máquina virtual (VM), talvez seja necessário monitorar as VMs para analisar e solucionar a causa. As VMs ficam disponíveis quando os clusters do vCenter Server e do ONTAP que hospedam o armazenamento de VM são adicionados ao Unified Manager.

Você vê os detalhes das VMs na página **VMware > > máquinas virtuais**. Informações, como disponibilidade, status, capacidade usada e alocada, latência de rede e IOPS e latência da VM, armazenamento de dados e host são exibidas. Para uma VM com suporte a vários datastores, a grade mostra as métricas do datastore com a pior latência, com um ícone de asterisco (\*) indicando datastores adicionais. Se você clicar no ícone, as métricas do datastore adicional serão exibidas. Algumas dessas colunas não estão disponíveis para classificação e filtragem.



Para visualizar uma VM e seus detalhes, a descoberta (polling ou coleta de métricas) do cluster do ONTAP deve estar concluída. Se o cluster for removido do Unified Manager, a VM não estará mais disponível após o próximo ciclo de descoberta.

Nessa página, você também pode visualizar a topologia detalhada de uma VM, exibindo os componentes aos quais a VM está relacionada, por exemplo, o host, o disco virtual e o datastore conectado a ela. A visualização de topologia exibe os componentes subjacentes em suas camadas específicas, na seguinte ordem: **Virtual Disk > VM > Host > Network > datastore > VMDK**.

Você pode determinar o caminho de e/S e latências em nível de componente de um aspecto topológico e identificar se o storage é a causa do problema de performance. A exibição de resumo da topologia exibe o caminho de e/S e destaca o componente que tem problemas de IOPS e latência para você decidir sobre as etapas de solução de problemas. Você também pode ter uma visualização expandida da topologia que mostra cada componente separadamente, juntamente com a latência desse componente. Você pode selecionar um componente para determinar o caminho de e/S destacado através das camadas.

## Exibindo a topologia de resumo

Para determinar problemas de performance visualizando as VMs em uma topologia de resumo:

1. Vá para **VMware > máquinas virtuais**.
2. PESQUISE sua VM digitando o nome na caixa de pesquisa. Você também pode filtrar seus resultados de pesquisa com base em critérios específicos clicando no botão **filtro**. No entanto, se você não conseguir encontrar sua VM, verifique se o vCenter Server correspondente foi adicionado e descoberto.



O vCenter Servers permite caracteres especiais (como %, &, \*, dólar, número, em, !, /, :, \*, ?, ", ", >, |, ;, ") nos nomes de entidades do vSphere, como VM, cluster, datastore, pasta ou arquivo. O VMware vCenter Server e o ESX/ESXi Server não escapam aos caracteres especiais usados nos nomes de exibição. No entanto, quando o nome é processado no Unified Manager, ele é exibido de forma diferente. Por exemplo, uma VM nomeada como %\$VC\_AIQUM\_clone\_191124% no vCenter Server é exibida como %25\$VC\_AIQUM\_clone\_191124%25 no Unified Manager. Você deve manter uma nota desse problema quando você consulta uma VM com um nome com caracteres especiais nela.

3. Verifique o status da VM. Os status da VM são recuperados do vCenter Server. Estão disponíveis os seguintes Estados. Para obter mais informações sobre esses status, consulte a documentação da VMware.
  - Normal
  - Aviso
  - Alerta
  - Não monitorizado
  - Desconhecido
4. Clique na seta para baixo ao lado da VM para ver a visualização de resumo da topologia dos componentes nas camadas de computação, rede e armazenamento. O nó que tem problemas de latência é destacado. A exibição de resumo exibe a pior latência dos componentes. Por exemplo, se uma VM tiver mais de um disco virtual, essa exibição exibirá o disco virtual que tem a pior latência entre todos os discos virtuais.
5. Para analisar a latência e a taxa de transferência do datastore durante um período de tempo, clique no botão **Workload Analyzer** na parte superior do ícone do objeto datastore. Vá para a página análise de workload, onde você pode selecionar um intervalo de tempo e exibir os gráficos de desempenho do datastore. Para obter mais informações sobre o analisador de carga de trabalho, consulte *Troubleshooting cargas de trabalho usando o analisador de carga de trabalho*.

## Visualização da topologia expandida

Você pode detalhar cada componente separadamente visualizando a topologia expandida da VM.

### Passos

1. Na visualização de topologia de resumo, clique em **expandir topologia**. Você pode ver a topologia detalhada de cada componente separadamente com os números de latência para cada objeto. Se houver vários nós em uma categoria, por exemplo, vários nós no datastore ou VMDK, o nó com pior latência será realçado em vermelho.
2. Para verificar o caminho de e/S de um objeto específico, clique nesse objeto para ver o caminho de e/S e o mapeamento correspondente. Por exemplo, para ver o mapeamento de um disco virtual, clique no disco virtual para visualizar o mapeamento realçado para o respectivo VMDK. No caso de um atraso de desempenho desses componentes, você pode coletar mais dados do ONTAP e solucionar o problema.



As métricas não são relatadas para VMDKs. Na topologia, apenas os nomes VMDK são exibidos, e não as métricas.

## Informações relacionadas

["Solução de problemas de workloads usando o analisador de workload"](#)

## Visualização da infraestrutura virtual em uma configuração de recuperação de desastres

Você pode visualizar as métricas de configuração e performance dos datastores hospedados em uma configuração do MetroCluster ou na configuração de recuperação de desastres (SVM DR) de máquina virtual de storage (Storage VM).

No Unified Manager, você pode visualizar os volumes nas ou LUNs em uma configuração do MetroCluster que são anexados como datastores no vCenter Server. Os datastores hospedados em uma configuração MetroCluster são representados na mesma visualização topológica que um datastore em um ambiente padrão.

Você também pode visualizar os volumes nas ou LUNs em uma configuração de recuperação de desastres da VM de storage que é mapeada para os datastores no vCenter Server.

## Visualização de datastores na configuração do MetroCluster

Observe os seguintes pré-requisitos antes de visualizar datastores em uma configuração do MetroCluster:

- Em caso de switchover e switchback, a descoberta dos clusters primário e secundário do par de HA e do vCenter Servers deve ser concluída.
- Os clusters primário e secundário do par de HA e vCenter Servers precisam ser gerenciados pelo Unified Manager.
- A configuração necessária deve ser concluída no ONTAP e no vCenter Server. Para obter informações, consulte a documentação do ONTAP e do vCenter.

["Centro de Documentação do ONTAP 9"](#)

Siga estas etapas para visualizar armazenamentos de dados:

1. Na página **VMware > máquinas virtuais**, clique na VM que hospeda o datastore. Clique no link **Workload Analyzer** ou no objeto datastore. No cenário padrão, quando o site principal que hospeda o volume ou LUN está funcionando como esperado, você pode ver os detalhes do cluster do SVM do site principal.
2. Em caso de desastre e um switchover consecutivo para o local secundário, o link do armazenamento de dados aponta para as métricas de desempenho do volume ou LUN no cluster secundário. Isso é refletido

depois que o próximo ciclo de clusters e a descoberta de SVM (aquisição) é concluída.

3. Depois de um switchback bem-sucedido, o link do datastore reflete novamente as métricas de desempenho do volume ou LUN no cluster primário. Isso é refletido depois que o próximo ciclo de clusters e a descoberta de SVM estiver concluída.

## Visualização de armazenamentos de dados na configuração de recuperação de desastres da VM de storage

Observe os seguintes pré-requisitos antes de visualizar armazenamentos de dados em uma configuração de recuperação de desastres da VM de storage:

- Em caso de switchover e switchback, a descoberta dos clusters primário e secundário do par de HA e do vCenter Servers deve ser concluída.
- Tanto o cluster de origem quanto o de destino e os pares de VM de storage devem ser gerenciados pelo Unified Manager.
- A configuração necessária deve ser concluída no ONTAP e no vCenter Server.
  - Para armazenamentos de dados nas (NFS e VMFS), em caso de desastre, as etapas incluem a criação da VM de storage secundário, a verificação das LIFs e rotas de dados, o estabelecimento de conexões perdidas no vCenter Server e a inicialização das VMs.

Para um switchback para o site principal, os dados entre os volumes devem ser sincronizados antes que o site principal comece a fornecer os dados.

- Para armazenamentos de dados SAN (iSCSI e FC para VMFS), o vCenter Server formata o LUN montado em um formato VMFS. Em caso de desastre, as etapas incluem a criação da VM de storage secundário, a verificação das LIFs e rotas de dados. Se os IPs de destino iSCSI forem diferentes dos LIFs primários, eles precisam ser adicionados manualmente. Os novos LUNs devem estar disponíveis como dispositivos sob o adaptador iSCSI do adaptador de armazenamento do host. Depois disso, novos datastores VMFS com as novas LUNs devem ser criados e as VMs antigas registradas com novos nomes. As VMs devem estar ativas e em funcionamento.

Em caso de recuperação, os dados entre os volumes devem ser sincronizados. Novos datastores VMFS devem ser criados novamente usando as LUNs e as VMs antigas registradas com novos nomes.

Para obter informações sobre a configuração, consulte a documentação do ONTAP e do vCenter Server.

### ["Centro de Documentação do ONTAP 9"](#)

Siga estas etapas para visualizar armazenamentos de dados:

1. Na página **VMware > máquinas virtuais**, clique no inventário da VM que hospeda o datastore. Clique no link do objeto datastore. No cenário padrão, você pode ver os dados de performance dos volumes e LUNs na VM de storage primário.
2. Em caso de desastre e um switchover consecutivo para a VM de storage secundário, o link do armazenamento de dados aponta para as métricas de desempenho do volume ou LUN na VM de storage secundário. Isso é refletido depois que o próximo ciclo de clusters e a descoberta de SVM (aquisição) é concluída.
3. Depois de um switchback bem-sucedido, o link do datastore reflete novamente as métricas de desempenho do volume ou LUN na VM de storage primário. Isso é refletido depois que o próximo ciclo de

clusters e a descoberta de SVM estiver concluída.

## Cenários não suportados

- Para uma configuração do MetroCluster, observe as seguintes limitações:
  - Aglomerados em apenas os NORMAL estados e SWITCHOVER são ocupados. outros estados, como PARTIAL\_SWITCHOVER, PARTIAL\_SWITCHBACK, e NOT\_REACHABLE não são suportados.
  - A menos que o comutador automático (ASO) esteja ativado, se o cluster primário cair, o cluster secundário não pode ser descoberto e a topologia continua a apontar para o volume ou LUN no cluster primário.
- Para uma configuração de recuperação de desastres de VM de armazenamento, observe a seguinte limitação:
  - Não é suportada uma configuração com o Site Recovery Manager (SRM) ou o Storage Replication Adapter (SRA) ativado para um ambiente de armazenamento SAN.

## Provisionamento e gerenciamento de workloads

O recurso de gerenciamento ativo do Active IQ Unified Manager fornece níveis de serviço de performance, políticas de eficiência de storage e APIs do fornecedor de storage para provisionar, monitorar e gerenciar workloads de storage em um data center.



O Unified Manager fornece essa funcionalidade por padrão. Você pode desativá-lo em **Gerenciamento de armazenamento > Configurações de recurso** se você não planeja usar essa funcionalidade.

Quando ativado, você pode provisionar workloads nos clusters do ONTAP gerenciados por sua instância do Unified Manager. Você também pode atribuir políticas, como níveis de Serviço de Performance e políticas de eficiência de storage, nos workloads e gerenciar seu ambiente de storage com base nessas políticas.

Este recurso ativa as seguintes funções:

- Detecção automática de workloads de storage nos clusters adicionados, o que possibilita a avaliação e implantação fáceis do workload de storage
- Provisionamento de workloads nas compatíveis com protocolos NFS e CIFS
- Provisionamento de workloads SAN compatíveis com protocolos iSCSI e FCP
- Suporte para protocolos NFS e CIFS no mesmo compartilhamento de arquivos
- Gerenciamento de níveis de serviço de performance e políticas de eficiência de storage
- Atribuição de níveis de serviço de performance e políticas de eficiência de storage a workloads de storage

As opções **Provisioning, Storage > cargas de trabalho** e **Policies** no painel esquerdo da IU permitem modificar várias configurações.

Você pode executar as seguintes funções usando estas opções:

- Veja as cargas de trabalho de armazenamento na página **Storage > cargas de trabalho**
- Crie workloads de storage a partir da página provisionar workloads de workload
- Crie e gerencie níveis de Serviço de Performance a partir de políticas

- Crie e gerencie políticas de eficiência de storage a partir de políticas
- Atribua políticas a workloads de storage a partir da página workloads

## Informações relacionadas

["Gerenciamento de storage baseado em políticas"](#)

## Visão geral dos workloads

Um workload representa as operações de entrada/saída (e/S) de um objeto de storage, como um volume ou LUN. A maneira como o storage é provisionado é baseada nos requisitos de workload esperados. As estatísticas de workload são controladas pelo Active IQ Unified Manager somente depois que houver tráfego de e para o objeto de storage. Por exemplo, os valores de IOPS e latência do workload ficam disponíveis depois que os usuários começam a usar um banco de dados ou um aplicativo de e-mail.

A página workloads exibe um resumo dos workloads de storage dos clusters do ONTAP gerenciados pelo Unified Manager. Ele fornece informações gerais cumulativas sobre os workloads de storage que estão em conformidade com o nível de Serviço de Performance e com os workloads de storage que não estão em conformidade. Ele também permite avaliar a capacidade e a performance (IOPS) totais, disponíveis e usadas dos clusters no data center.



Recomenda-se que você avalie o número de workloads de storage que não estão em conformidade, não estão disponíveis ou não gerenciados por nenhum nível de Serviço de Performance e tome as medidas necessárias para garantir a conformidade, o uso da capacidade e o IOPS.

A página cargas de trabalho tem as duas seções a seguir:

- **Visão geral de workloads:** Fornece uma visão geral do número de workloads de storage nos clusters do ONTAP gerenciados pelo Unified Manager.
- **Visão geral do data center:** Fornece uma visão geral da capacidade e IOPS dos workloads de storage no data center. Os dados relevantes são exibidos em um nível de data center e para o indivíduo .

## Seção de visão geral das cargas de trabalho

A seção visão geral de cargas de trabalho fornece informações gerais cumulativas sobre as cargas de trabalho de storage. O status dos workloads de storage é exibido com base nos níveis de Serviço de desempenho atribuídos e não atribuídos.

- **Assigned:** Os seguintes status são relatados para cargas de trabalho de armazenamento nas quais os níveis de Serviço de desempenho foram atribuídos:
  - **Conformidade:** O desempenho dos workloads de storage é baseado nos níveis de Serviço de desempenho atribuídos a eles. Se os workloads de storage estiverem dentro do limite de latência definido nos níveis de Serviço de desempenho associados, eles serão marcados como "conformes". Os workloads conformes são marcados em azul.
  - **Não-conforme:** Durante o monitoramento de desempenho, os workloads de storage são marcados como "não-conformes" se a latência dos workloads de storage exceder o limite de latência definido no nível de Serviço de desempenho associado. Os workloads que não estão em conformidade são marcados com laranja.

- **Indisponível:** As cargas de trabalho de armazenamento são marcadas como "indisponíveis" se estiverem offline ou se o cluster correspondente não estiver acessível. As cargas de trabalho indisponíveis estão marcadas em vermelho.
- **Não atribuído:** Cargas de trabalho de armazenamento que não tenham um nível de Serviço de desempenho atribuído a elas, são relatadas como ""não atribuídas"". O número é transmitido pelo ícone de informação.

A contagem total de workloads é a soma total das cargas de trabalho atribuídas e não atribuídas.

Você pode clicar no número total de cargas de trabalho exibidas nesta seção e visualizá-las na página cargas de trabalho.

A subseção conformidade por níveis de serviço de desempenho exibe o número total de cargas de trabalho de storage disponíveis:

- Em conformidade com cada tipo de nível de Serviço de Performance
- Para a qual há uma incompatibilidade entre os níveis de Serviço de desempenho atribuídos e recomendados

### Seção de visão geral do data center

A seção de visão geral do data center representa graficamente a capacidade disponível e usada e as IOPS de todos os clusters no data center. Usando esses dados, você deve gerenciar a capacidade e o IOPS dos workloads de storage. A seção também exibe as seguintes informações para os workloads de storage em todos os clusters:

- A capacidade total, disponível e usada de todos os clusters no data center
- O total, disponível e usado IOPS em todos os clusters no data center
- A capacidade disponível e usada com base em cada nível de Serviço de Performance
- O IOPS disponível e usado com base em cada nível de serviço de performance
- O espaço total e o IOPS usados pelos workloads que não têm nível de Serviço de Performance atribuído

### Como a capacidade e o desempenho do data center são calculados com base nos níveis de Serviço de desempenho

A capacidade usada e o IOPS são recuperados em termos da capacidade total usada e da performance de todos os workloads de storage nos clusters.

O IOPS disponível é calculado com base na latência esperada e nos níveis de Serviço de desempenho recomendados nos nós. Ele inclui o IOPS disponível para todos os níveis de serviço de performance cuja latência esperada é menor ou igual à sua própria latência esperada.

A capacidade disponível é calculada com base na latência esperada e nos níveis de Serviço de desempenho recomendados em agregados. Ele inclui a capacidade disponível para todos os níveis de Serviço de Performance cuja latência esperada é menor ou igual a sua própria latência esperada.

### Visualização de workloads

Quando você adiciona clusters ao Unified Manager, os workloads de storage em cada cluster são automaticamente descobertos e exibidos na página cargas de trabalho.

O Unified Manager começa a analisar os workloads para recomendação (PSLs recomendadas) somente após



o início das operações de e/S nos workloads de storage.

Os volumes FlexGroup e seus componentes estão excluídos.

### Visão geral dos workloads

A página Visão geral das cargas de trabalho exibe a visão geral das cargas de trabalho no data center e a visão geral de espaço e desempenho do data center.

- **Painel Visão geral das cargas de trabalho:** Exibe o número total de cargas de trabalho e o número de cargas de trabalho com ou sem PSLs atribuídas a elas. A separação da contagem de carga de trabalho para cada PSL também é exibida. Clicar nas contagens leva você para a visualização **todas as cargas de trabalho** com as cargas de trabalho filtradas. Você também pode ver o número de cargas de trabalho que não estão em conformidade com a recomendação do sistema e atribuir as PSLs recomendadas pelo sistema a elas clicando no botão **Assign System-Recommended PSLs** (atribuir PSLs recomendados pelo sistema).
- **Painel de Visão geral do data center:** Exibe o espaço disponível e usado (TIB) e o desempenho (IOPS) do data center. Também é exibida uma separação entre o espaço disponível e usado (TIB) e o desempenho (IOPS) de todos os workloads em cada PSL.

### Visualização de todos os workloads

A página **armazenamento > cargas de trabalho > todas as cargas de trabalho** lista as cargas de trabalho de armazenamento associadas aos clusters do ONTAP gerenciados pelo Unified Manager.

Para as cargas de trabalho de storage recém-descobertas nas quais não houve operações de e/S, o status é "aguardando pela e/S". Depois que as operações de e/S começam nas cargas de trabalho de storage, o Unified Manager inicia a análise e o status da carga de trabalho muda para "Learning...". Após a conclusão da análise (dentro de 24 horas a partir do início das operações de e/S), as PSLs recomendadas são exibidas para as cargas de trabalho de storage.

A página também permite que você atribua políticas de eficiência de storage (SEPs) e níveis de serviço de performance (PSLs) a workloads de storage. Você pode executar várias tarefas:

- Adicionar ou provisionar workloads de storage
- Visualize e filtre a lista de cargas de trabalho
- Atribuir PSLs a workloads de storage
- Avalie as PSLs recomendadas pelo sistema e atribua-as a cargas de trabalho
- Atribuir SEPs a workloads de storage

### Adição ou provisionamento de workloads de storage

Você pode adicionar ou provisionar os workloads de storage a LUNs compatíveis (compatíveis com protocolos iSCSI e FCP), compartilhamentos de arquivos NFS e compartilhamentos de SMB.

#### Passos

1. Clique em **armazenamento > cargas de trabalho > todas as cargas de trabalho > criar**.
2. Crie workloads. Para obter informações, "[Provisionamento e gerenciamento de workloads](#)" consulte .

### Visualização e filtragem de workloads

Na tela todos os workloads, você pode visualizar todos os workloads no data center ou pesquisar workloads

de storage específicos com base nas PSLs ou nos nomes deles. Pode utilizar o ícone de filtro para introduzir condições específicas para a sua pesquisa. Você pode pesquisar por diferentes condições de filtro, como pelo cluster de host ou VM de armazenamento. A opção **Capacity Total** permite a filtragem pela capacidade total das cargas de trabalho (por MB). No entanto, nesse caso, o número de cargas de trabalho retornadas pode variar, porque a capacidade total é comparada em um nível de byte.

Para cada carga de trabalho, são exibidas informações, como o cluster de host e a VM de armazenamento, juntamente com o PSL e o SEP atribuídos.

A página também permite visualizar os detalhes de performance de um workload. Você pode exibir informações detalhadas sobre o IOPS, a capacidade e a latência da carga de trabalho clicando no botão **escolher / pedir colunas** e selecionando colunas específicas para exibir. A coluna Exibição de desempenho exibe as IOPS média e pico de uma carga de trabalho e você pode clicar no ícone do analisador de carga de trabalho para exibir a análise detalhada de IOPS.

### **Análise de critérios de performance e capacidade de um workload**

O botão **Analyze Workload** (analisar carga de trabalho) na janela pop-up **IOPS Analysis** (análise de carga de trabalho) leva você à página Workload Analysis (análise de carga de trabalho), onde você pode selecionar um intervalo de tempo e exibir as tendências de latência, taxa de transferência e capacidade para a carga de trabalho selecionada. Para obter mais informações sobre o analisador de carga de trabalho, "[Solução de problemas de cargas de trabalho usando o analisador de carga de trabalho](#)" consulte .

Você pode exibir informações de desempenho sobre uma carga de trabalho para ajudar na solução de problemas clicando no ícone do gráfico de barras na coluna **Exibição de desempenho**. Para visualizar gráficos de desempenho e capacidade na página análise de workload para analisar o objeto, clique no botão **Analyze Workload**.

Para obter mais informações, "[Quais dados o analisador de carga de trabalho exibe](#)" consulte .

### **Atribuindo políticas a cargas de trabalho**

Você pode atribuir políticas de eficiência de storage (SEPs) e níveis de serviço de performance (PSLs) a workloads de storage na página todos os workloads usando as diferentes opções de navegação.

#### **Atribuição de políticas a uma única carga de trabalho**

Você pode atribuir um PSL ou um SEP ou ambos a uma única carga de trabalho. Siga estes passos:

1. Selecione a carga de trabalho.
2. Clique no ícone de edição ao lado da linha e, em seguida, clique em **Editar**.

Os campos **nível de Serviço de desempenho atribuído** e **Política de eficiência de armazenamento** estão ativados.

3. Selecione o PSL ou SEP pretendido ou ambos.
4. Clique no ícone de verificação para aplicar as alterações.



Você também pode selecionar uma carga de trabalho e clicar em **mais ações** para atribuir as políticas.

## Atribuição de políticas a vários workloads de storage

Você pode atribuir uma PSL ou uma SEP a vários workloads de storage juntos. Siga estes passos:

1. Marque as caixas de seleção das cargas de trabalho às quais você deseja atribuir a política ou selecione todas as cargas de trabalho em seu data center.
2. Clique em **mais ações**.
3. Para atribuir um PSL, selecione **Assign Performance Service Level**. Para atribuir uma SEP, selecione **Assign Storage Efficiency Policy**. É apresentado um pop-up para selecionar a política.
4. Selecione a política apropriada e clique em **Apply**. O número de cargas de trabalho nas quais as políticas são atribuídas é exibido. As cargas de trabalho nas quais as políticas não são atribuídas também são listadas, com a causa.



A aplicação de políticas em cargas de trabalho em massa pode levar algum tempo, dependendo do número de cargas de trabalho selecionadas. Você pode clicar no botão **Executar em segundo plano** e continuar com outras tarefas enquanto a operação é executada em segundo plano. Quando a atribuição em massa estiver concluída, você poderá exibir o status de conclusão. Se você estiver aplicando um PSL em várias cargas de trabalho, não poderá acionar outra solicitação quando a tarefa anterior de atribuição em massa estiver em execução.

## Atribuição de PSLs recomendadas pelo sistema a cargas de trabalho

Você pode atribuir PSLs recomendados pelo sistema a essas cargas de trabalho de storage em um data center que não tenha PSLs atribuídas ou as PSLs atribuídas não correspondem à recomendação do sistema. Para usar essa funcionalidade, clique no botão **Assign System Recommended PSLs** (atribuir PSLs recomendados pelo sistema). Não é necessário selecionar cargas de trabalho específicas.

A recomendação é determinada internamente pela análise do sistema e é ignorada para as cargas de trabalho cujos IOPS e outros parâmetros não coincidem com as definições de qualquer PSL disponível. Os workloads de storage com `Waiting for I/O` status e aprendizado também são excluídos.



Há palavras-chave especiais que o Unified Manager procura no nome da carga de trabalho para substituir a análise do sistema e recomendar um PSL diferente para a carga de trabalho. Quando a carga de trabalho tem as letras "ora" no nome, o **Extreme Performance** PSL é recomendado. E quando a carga de trabalho tem as letras "vm" no nome, o **Performance** PSL é recomendado.

Veja também o artigo da base de conhecimento (KB) ["O ActiveIQ Unified Manager "atribuir nível de serviço de performance recomendado pelo sistema" não é adaptável a um workload altamente variável"](#)

## Provisionar volumes de compartilhamento de arquivos

Você pode criar volumes de compartilhamento de arquivos compatíveis com os protocolos CIFS/SMB e NFS, em um cluster existente e Storage Virtual Machine (storage VM) na página provisionar workloads.

### Antes de começar

- A VM de storage deve ter espaço para provisionar o volume de compartilhamento de arquivos.
- Um ou ambos os serviços SMB e NFS devem estar ativados na VM de storage.

- Para selecionar e atribuir o nível de Serviço de desempenho (PSL) e a Política de eficiência de armazenamento (SEP) na carga de trabalho, as políticas devem ter sido criadas antes de começar a criar a carga de trabalho.

## Passos

1. Na página **provisione Workload**, adicione o nome da carga de trabalho que deseja criar e selecione o cluster na lista disponível.
2. Com base no cluster selecionado, o campo **STORAGE VM** filtra as VMs de ARMAZENAMENTO disponíveis para esse cluster. Selecione a VM de armazenamento necessária na lista.

Com base nos serviços SMB e NFS compatíveis com a VM de storage, a opção **nas** é ativada na seção informações do host.

3. Na seção armazenamento e otimização, atribua a capacidade de armazenamento e PSL e, opcionalmente, uma SEP para a carga de trabalho.

As especificações para a SEP são atribuídas ao LUN e as definições para a PSL são aplicadas à carga de trabalho quando é criada.

4. Marque a caixa de seleção **impor limites de desempenho** se desejar aplicar o PSL que você atribuiu à carga de trabalho.

A atribuição de um PSL a uma carga de trabalho garante que o agregado no qual a carga de trabalho é criada possa suportar os objetivos de desempenho e capacidade definidos na respectiva política. Por exemplo, se uma carga de trabalho for atribuída a "PSL de desempenho extremo", o agregado no qual a carga de trabalho deve ser provisionada deve ter a capacidade de suportar os objetivos de desempenho e capacidade da política de "desempenho extremo", como o armazenamento SSD.



A menos que você marque essa caixa de seleção, o PSL não será aplicado à carga de trabalho e o status da carga de trabalho no painel aparecerá como não atribuído.

5. Selecione a opção **nas**.

Se não conseguir ver a opção **nas** ativada, verifique se a VM de armazenamento selecionada suporta SMB ou NFS ou ambos.



Se a VM de storage estiver ativada para serviços SMB e NFS, você poderá selecionar as caixas de seleção **Share by NFS** e **Share by SMB** e criar um compartilhamento de arquivos compatível com protocolos NFS e SMB. Se quiser criar um compartilhamento SMB ou CIFS, marque apenas a caixa de seleção correspondente.

6. Para volumes de compartilhamento de arquivos NFS, especifique o endereço IP do host ou da rede para acessar o volume de compartilhamento de arquivos. Você pode inserir valores separados por vírgulas para vários hosts.

Ao adicionar o endereço IP do host, uma verificação interna é executada para corresponder os detalhes do host com a VM de armazenamento e a política de exportação para esse host é criada, ou no caso de haver uma política existente, ela é reutilizada. Se houver vários compartilhamentos NFS criados para o mesmo host, uma política de exportação disponível para o mesmo host com regras correspondentes será reutilizada para todos os compartilhamentos de arquivos. A função de especificar regras de políticas individuais ou reutilizar políticas fornecendo chaves de política específicas está disponível quando você provisiona o compartilhamento NFS usando APIs.

7. Para um compartilhamento SMB, especifique quais usuários ou grupos de usuários podem acessar o compartilhamento SMB e atribuir as permissões necessárias. Para cada grupo de usuários, uma nova lista de controle de acesso (ACL) é gerada durante a criação do compartilhamento de arquivos.
8. Clique em **Salvar**.

O workload é adicionado à lista de workloads de storage.

## Provisionamento de LUNs

Você pode criar LUNs compatíveis com os protocolos CIFS/SMB e NFS, em um cluster existente e Storage Virtual Machine (storage VM) na página provisionar Workload.

### Antes de começar

- A VM de storage deve ter espaço para provisionar o LUN.
- Tanto o iSCSI como o FCP devem estar ativados na VM de storage na qual você cria o LUN.
- Para selecionar e atribuir o nível de Serviço de desempenho (PSL) e a Política de eficiência de armazenamento (SEP) na carga de trabalho, as políticas devem ter sido criadas antes de começar a criar a carga de trabalho.

### Passos

1. Na página **provisione Workload**, adicione o nome da carga de trabalho que deseja criar e selecione o cluster na lista disponível.

Com base no cluster selecionado, o campo **STORAGE VM** filtra as VMs de ARMAZENAMENTO disponíveis para esse cluster.

2. Selecione a VM de armazenamento na lista que suporta os serviços iSCSI e FCP.

Com base na sua seleção, a opção SAN está ativada na seção informações do anfitrião.

3. Na seção **Storage and Optimization**, atribua a capacidade de armazenamento e PSL e, opcionalmente, o SEP para a carga de trabalho.

As especificações para a SEP são atribuídas ao LUN e as definições para a PSL são aplicadas à carga de trabalho quando é criada.

4. Marque a caixa de seleção **impor limites de desempenho** se desejar aplicar o PSL atribuído na carga de trabalho.

A atribuição de um PSL a uma carga de trabalho garante que o agregado no qual a carga de trabalho é criada possa suportar os objetivos de desempenho e capacidade definidos na respectiva política. Por exemplo, se um workload recebe o PSL de "desempenho extremo", o agregado no qual o workload deve ser provisionado deve ter a capacidade de suportar os objetivos de desempenho e capacidade da política de "desempenho extremo", como o storage SSD.



A menos que você marque essa caixa de seleção, o PSL não será aplicado à carga de trabalho e o status da carga de trabalho no painel será exibido como `unassigned`.

5. Selecione a opção **SAN**. Se não conseguir ver a opção **SAN** ativada, verifique se a VM de armazenamento selecionada suporta iSCSI e FCP.
6. Selecione o sistema operacional do host.

7. Especifique o mapeamento do host para controlar o acesso dos iniciadores ao LUN. Você pode atribuir grupos de iniciadores existentes (grupos de iniciadores) ou definir e mapear novos grupos de iniciadores.



Se você criar um novo grupo ao provisionar o LUN, precisará esperar até o próximo ciclo de descoberta (até 15 minutos) para usá-lo. Portanto, é recomendável que você use um grupo existente da lista de grupos disponíveis.

Se você quiser criar um novo grupo de iniciadores, selecione o botão **criar um novo grupo de iniciadores** e insira as informações do grupo de iniciadores.

8. Clique em **Salvar**.

O LUN é adicionado à lista de cargas de trabalho de storage.

## Níveis de serviço de performance

Um nível de serviço de desempenho (PSL) permite definir os objetivos de desempenho e armazenamento de um workload. Você pode atribuir um PSL a uma carga de trabalho ao criar inicialmente a carga de trabalho ou depois editar a carga de trabalho.

O gerenciamento e o monitoramento de recursos de storage são baseados nos objetivos de nível de serviço (SLOs). Os SLOs são definidos por contratos de nível de serviço baseados no desempenho e na capacidade exigidos. No Gerenciador Unificado, os SLOs referem-se às definições de PSL dos aplicativos que estão sendo executados no storage NetApp. Os serviços de storage são diferenciados com base no desempenho e na utilização dos recursos subjacentes. Um PSL é uma descrição dos objetivos do serviço de storage. Um PSL permite que o provedor de storage especifique os objetivos de desempenho e capacidade para a carga de trabalho. Quando você atribui um PSL em um workload, o workload correspondente no ONTAP é gerenciado por seus objetivos de performance e capacidade. Cada PSL é regido por IOPs mínimos de pico, esperados e absolutos e latência esperada.

O Unified Manager tem os seguintes tipos de PSLs:

- **Definido pelo sistema:** O Unified Manager fornece algumas políticas enlatadas que não podem ser alteradas. Estas PSLs predefinidas são:

- Performance extrema
- Desempenho
- Valor

As PSLs de performance, performance e valor extremas são aplicáveis à maioria dos workloads de storage comuns em um data center.

O Unified Manager também oferece três níveis de Performance Service para aplicações de banco de dados. Estes são PSLs de alto desempenho que suportam IOPS em expansão e são apropriados para aplicativos de banco de dados com a maior demanda de taxa de transferência.

- Extremo para Registros de banco de dados
  - Extremo para dados compartilhados de banco de dados
  - Extremo para dados de banco de dados
- **Definido pelo usuário:** Se os níveis de Serviço de desempenho predefinidos não atenderem aos seus requisitos, você poderá criar novas PSLs para atender às suas necessidades. Para obter informações,

"Criando e editando níveis de Serviço de desempenho" consulte .

- **Beyond Extreme:** As PSLs Beyond Extreme são as PSLs recomendadas pelo sistema que são sugeridas para cargas de trabalho que exigem IOPs superiores ao Extreme. As cargas de trabalho são analisadas internamente com base em suas IOPS, capacidade e latência, e um Beyond Extreme PSL é recomendado para cada uma dessas cargas de trabalho na tela **Storage > cargas de trabalho > todas as cargas de trabalho**. Você pode aplicar as PSLs às cargas de trabalho para garantir um desempenho ideal.

Os parâmetros IOPs para as cargas de trabalho são gerados dinamicamente, dependendo do comportamento da carga de trabalho, e anexados ao nome do Beyond Extreme PSL no formato `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`. Por exemplo, se o sistema determinar uma carga de trabalho para ter IOPs de pico e esperados como 106345 37929 e respectivamente, o Beyond Extreme PSL gerado para a carga de trabalho é nomeado como `Beyond Extreme 106345 37929`. Embora essas PSLs sejam recomendadas pelo sistema, quando você as atribui a cargas de trabalho, essas PSLs são rotuladas como `User-defined` no tipo.

## Gerenciamento de workloads atribuindo PSLs

Pode acessar as PSLs a partir da página **Políticas > Performance Service Levels** e utilizando as APIs do fornecedor de armazenamento. Gerenciar workloads de storage atribuindo PSLs a eles é conveniente, pois você não precisa gerenciar individualmente os workloads de storage. Quaisquer modificações também podem ser gerenciadas reatribuindo outro PSL em vez de gerenciá-los individualmente. O Unified Manager ajuda você a atribuir PSLs em seus workloads com base em avaliações e recomendações internas.

Para obter informações sobre como atribuir PSLs recomendadas pelo sistema a cargas de trabalho, consulte ["Atribuição de PSLs recomendadas pelo sistema a cargas de trabalho"](#)

A página níveis de Serviço de desempenho lista as políticas PSL disponíveis e permite que você as adicione, edite e exclua.



Não é possível modificar um PSL definido pelo sistema ou que está atualmente atribuído a uma carga de trabalho. Não é possível excluir um PSL atribuído a uma carga de trabalho ou se for o único PSL disponível.

Esta página exibe as seguintes informações:

Campo	Descrição
Nome	Nome do PSL.
Tipo	Se a política é definida pelo sistema ou definida pelo usuário.
IOPS/TB esperados	Número mínimo de IOPS que um aplicativo deve executar em um LUN ou compartilhamento de arquivos. IOPS esperado especifica o mínimo esperado alocado, com base no tamanho alocado do objeto de storage.

Campo	Descrição
IOPS/TB de pico	<p>Número máximo de IOPS que um aplicativo pode executar em um LUN ou compartilhamento de arquivos. IOPS de pico especifica o máximo possível alocado, com base no tamanho alocado do objeto de armazenamento ou no tamanho usado do objeto de armazenamento.</p> <p>IOPS de pico são baseados em uma política de alocação. A política de alocação é alocada-espaço ou espaço usado. Quando a política de alocação é definida como espaço alocado, o IOPS de pico é calculado com base no tamanho do objeto de storage. Quando a política de alocação é definida como espaço usado, o IOPS de pico é calculado com base na quantidade de dados armazenados no objeto de storage, levando em consideração as eficiências de storage. Por padrão, a política de alocação é definida como espaço usado.</p>
IOPS mínimo absoluto	<p>O IOPS mínimo absoluto é usado como uma substituição, quando o IOPS esperado é menor do que esse valor. Os valores padrão das PSLs definidas pelo sistema são os seguintes:</p> <ul style="list-style-type: none"> <li>• Desempenho extremo: Se o IOPS esperado &gt; 6144/TB, o IOPS mínimo absoluto é 1000</li> <li>• Desempenho: Se o IOPS esperado for superior a 2048/TB e inferior a 6144/TB, o IOPS mínimo absoluto é 500</li> <li>• Valor: Se IOPS esperado &gt; 128/TB e inferior a 2048/TB, então IOPS mínimo absoluto é 75</li> </ul> <p>Os valores padrão das PSLs de banco de dados definidas pelo sistema são os seguintes:</p> <ul style="list-style-type: none"> <li>• Extreme for Database Logs: Se IOPS esperado &gt; 22528, então IOPS mínimo absoluto é 4000</li> <li>• Extremo para dados compartilhados de banco de dados: Se IOPS esperado &gt; 16384, então IOPS mínimo absoluto é 2000</li> <li>• Extremo para dados de banco de dados: Se o IOPS esperado &gt; 12288, o IOPS mínimo absoluto é 2000</li> </ul> <p>O valor mais alto do IOPS mínimo absoluto para PSLs personalizadas pode ser de no máximo 75000. O valor mais baixo é calculado da seguinte forma:</p> <p>1000 ms/latência esperada</p>



<b>Campo</b>	<b>Descrição</b>
Latência esperada	Latência esperada para IOPS do storage em milissegundos por operação (ms/op).
Capacidade	Capacidade total disponível e usada nos clusters.
Workloads	Número de cargas de trabalho de armazenamento que foram atribuídas ao PSL.

Para obter informações sobre como o IOPS de pico e os IOPs esperados ajudam a alcançar desempenho diferenciado consistente em clusters do ONTAP, consulte o seguinte artigo da KB: ["O que é orçamento de desempenho?"](#)

#### **Eventos gerados para cargas de trabalho que ultrapassam o limite definido pelas PSLs**

Observe que se as cargas de trabalho excederem o valor de latência esperado por 30% do tempo durante a hora anterior, o Unified Manager gerará um dos eventos a seguir para notificá-lo de um possível problema de desempenho:

- Limite de latência de volume de workload violado conforme definido pela Política de nível de Serviço de Performance
- Limite de latência LUN do workload violado conforme definido pela Política de nível de Serviço de Performance.

Você pode querer analisar a carga de trabalho para ver o que pode estar causando os valores de latência mais altos.

Para obter mais informações, consulte os seguintes links:

- ["Eventos de volume"](#)
- ["O que acontece quando uma política de limite de desempenho é violada"](#)
- ["Como o Unified Manager usa a latência do workload para identificar problemas de performance"](#)
- ["Quais são os eventos de desempenho"](#)

#### **PSLs definidas pelo sistema**

A tabela a seguir fornece informações sobre as PSLs definidas pelo sistema:

<b>Nível de Serviço de desempenho</b>	<b>Descrição e caso de uso</b>	<b>Latência esperada (ms/op)</b>	<b>IOPS de pico</b>	<b>IOPS esperado</b>	<b>IOPS mínimo absoluto</b>
Performance extrema	<p>Fornece taxa de transferência extremamente alta a uma latência muito baixa</p> <p>Ideal para aplicações sensíveis à latência</p>	1	12288	6144	1000
Desempenho	<p>Fornece alta taxa de transferência com baixa latência</p> <p>Ideal para bancos de dados e aplicações virtualizadas</p>	2	4096	2048	500
Valor	<p>Fornece alta capacidade de armazenamento e latência moderada</p> <p>Ideal para aplicativos de alta capacidade, como e-mail, conteúdo da Web, compartilhamentos de arquivos e destinos de backup</p>	17	512	128	75

Nível de Serviço de desempenho	Descrição e caso de uso	Latência esperada (ms/op)	IOPS de pico	IOPS esperado	IOPS mínimo absoluto
Extremo para Registros de banco de dados	<p>Fornece taxa de transferência máxima com a menor latência.</p> <p>Ideal para aplicações de base de dados que suportam registros de bases de dados. Este PSL fornece o throughput mais alto porque os logs do banco de dados são extremamente bursty e o Registro está constantemente em demanda.</p>	1	45056	22528	4000
Extremo para dados compartilhados de banco de dados	<p>Fornece taxa de transferência muito alta com a menor latência.</p> <p>Ideal para dados de aplicativos de banco de dados que são armazenados em um armazenamento de dados comum, mas são compartilhados entre bancos de dados.</p>	1	32768	16384	2000

Nível de Serviço de desempenho	Descrição e caso de uso	Latência esperada (ms/op)	IOPS de pico	IOPS esperado	IOPS mínimo absoluto
Extremo para dados de banco de dados	<p>Fornecer alta taxa de transferência com a menor latência.</p> <p>Ideal para dados de aplicativos de banco de dados, como informações de tabela de banco de dados e metadados.</p>	1	24576	12288	2000

### Criando e editando níveis de Serviço de desempenho

Quando os níveis de Serviço de performance definidos pelo sistema não correspondem aos requisitos de workload, você pode criar seus próprios níveis de Serviço de performance otimizados para seus workloads.

#### Antes de começar

- Tem de ter a função Administrador de aplicações.
- O nome do nível de Serviço de desempenho deve ser exclusivo e você não pode usar as seguintes palavras-chave reservadas:

Prime Extreme, , Performance Value , Unassigned, , , Learning Idle, , , Default e None.

Você cria e edita níveis de Serviço de Performance personalizados na página níveis de Serviço de Performance definindo os objetivos de nível de serviço necessários para os aplicativos que acessarão o storage.



Não é possível modificar um nível de Serviço de Performance se ele estiver atualmente atribuído a uma carga de trabalho.

#### Passos

1. No painel de navegação à esquerda em **Settings**, selecione **Policies > Performance Service Levels**.
2. Na página **níveis de serviço de desempenho**, clique no botão apropriado, dependendo se você deseja criar um novo nível de serviço de desempenho ou se deseja editar um nível de serviço de desempenho existente.

Para...	Siga estes passos...
Crie um novo nível de Serviço de Performance	Clique em <b>Add</b> .

Para...	Siga estes passos...
Editar um nível de Serviço de desempenho existente	Selecione um nível de Serviço de desempenho existente e clique em <b>Editar</b> .

É apresentada a página para adicionar ou editar um nível de Serviço de desempenho.

3. Personalize o nível de Serviço de desempenho especificando os objetivos de desempenho e clique em **Enviar** para salvar o nível de Serviço de desempenho.

É possível aplicar o nível de Serviço de Performance novo ou alterado a workloads (LUNs, compartilhamentos de arquivos NFS, compartilhamentos CIFS) da página de workloads ou ao provisionar um novo workload.

## Gerenciamento de políticas de eficiência de storage

Uma Política de eficiência de storage (SEP) permite definir as características de eficiência de storage de um workload. Você pode atribuir uma SEP a uma carga de trabalho ao criar inicialmente a carga de trabalho ou depois editar a carga de trabalho.

A eficiência de storage inclui tecnologias como thin Provisioning, deduplicação e compressão de dados que aumentam a utilização do storage e diminuem os custos de storage. Ao criar SEPs, você pode usar essas tecnologias de economia de espaço individualmente ou em conjunto para obter a máxima eficiência de storage. Quando você associa as políticas aos workloads de storage, as configurações de política especificadas são atribuídas a elas. Com o Unified Manager, você pode atribuir SEPs definidos pelo sistema e definidos pelo usuário para otimizar os recursos de storage no data center.

O Unified Manager fornece dois SEPs definidos pelo sistema: Alto e baixo. Esses SEPs são aplicáveis à maioria das cargas de trabalho de storage em um data center. No entanto, você pode criar suas próprias políticas se os SEPs definidos pelo sistema não atenderem aos seus requisitos.

Não é possível modificar uma SEP definida pelo sistema ou que esteja atualmente atribuída a uma carga de trabalho. Não é possível excluir uma SEP atribuída a uma carga de trabalho ou se for a única SEP disponível.

A página políticas de eficiência de armazenamento lista os SEPs disponíveis e permite adicionar, editar e excluir SEPs personalizados. Esta página exibe as seguintes informações:

Campo	Descrição
Nome	Nome do SEP.
Tipo	Se a política é definida pelo sistema ou definida pelo usuário.
Reserva de espaço	Se o volume é de thin Provisioning ou de thin Provisioning.

<b>Campo</b>	<b>Descrição</b>
Deduplicação	<p>Se a deduplicação está ativada na carga de trabalho:</p> <ul style="list-style-type: none"> <li>• Inline: A deduplicação ocorre enquanto é gravada na carga de trabalho</li> <li>• Contexto: A deduplicação ocorre na carga de trabalho</li> <li>• Desativar: A deduplicação está desativada na carga de trabalho</li> </ul>
Compactação	<p>Se a compactação de dados está ativada na carga de trabalho:</p> <ul style="list-style-type: none"> <li>• Inline: A compactação de dados ocorre enquanto é gravada na carga de trabalho</li> <li>• Fundo: A compactação de dados ocorre na carga de trabalho</li> <li>• Desativar: A compressão de dados está desativada na carga de trabalho</li> </ul>
Workloads	Número de cargas de trabalho de storage que foram atribuídas à SEP

### **Diretrizes para criar uma política de eficiência de storage personalizada**

Se os SEPs existentes não atenderem aos requisitos de política para suas cargas de trabalho de storage, você poderá criar uma SEP personalizada. No entanto, é recomendável que você tente usar os SEPs definidos pelo sistema para suas cargas de trabalho de storage e apenas crie SEPs personalizados, se necessário.

Você pode exibir a SEP atribuída a cargas de trabalho na página todas as cargas de trabalho e na página de detalhes de volume / integridade. É possível visualizar a taxa de redução de dados no nível do cluster (sem cópias Snapshot) com base nessas eficiências de storage no painel de capacidade no painel e na visualização capacidade: Todos os clusters.

### **Criação e edição de políticas de eficiência de storage**

Quando as políticas de eficiência de storage definidas pelo sistema não correspondem aos requisitos de workload, você pode criar suas próprias políticas de eficiência de storage otimizadas para seus workloads.

#### **Antes de começar**

- Tem de ter a função Administrador de aplicações.
- O nome da Política de eficiência de armazenamento deve ser exclusivo e você não pode usar as seguintes palavras-chave reservadas:

High Low, , Unassigned Learning , Idle, , , Default, e None.

Você cria e edita políticas de eficiência de storage personalizadas na página políticas de eficiência de storage definindo as características de eficiência de storage necessárias para os aplicativos que acessarão o storage.



Não é possível modificar uma Política de eficiência de storage se ela estiver atualmente atribuída a uma carga de trabalho.

## Passos

1. No painel de navegação à esquerda em **Settings**, selecione **Policies > Storage Efficiency**.
2. Na página **políticas de eficiência de armazenamento**, clique no botão apropriado, dependendo se você deseja criar uma nova Política de eficiência de armazenamento ou se deseja editar uma Política de eficiência de armazenamento existente.

Para...	Siga estes passos...
Crie uma nova política de eficiência de storage	Clique em <b>Add</b>
Editar uma política de eficiência de storage existente	Selecione uma Política de eficiência de armazenamento existente e clique em <b>Editar</b>

A página para adicionar ou editar uma Política de eficiência de armazenamento é exibida.

3. Personalize a Política de eficiência de armazenamento especificando as características de eficiência de armazenamento e clique em **Enviar** para salvar a Política de eficiência de armazenamento.

Você pode aplicar a nova ou alterada Política de eficiência de storage a workloads (LUNs, compartilhamentos de arquivos NFS, compartilhamentos CIFS) da página de workloads ou ao provisionar um novo workload.

## Gerenciamento e monitoramento de configurações do MetroCluster

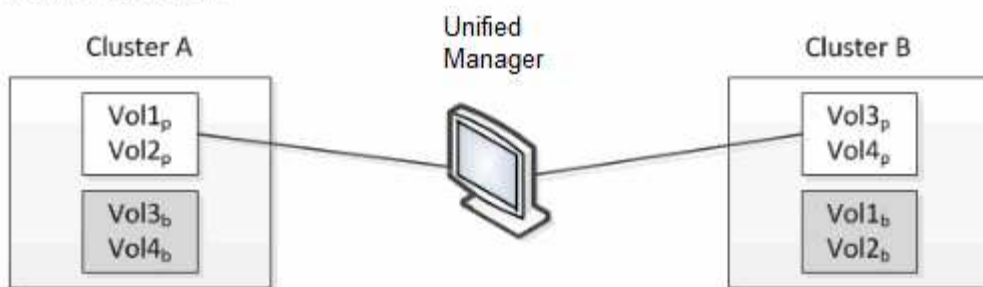
O suporte a monitoramento para configurações do MetroCluster na IU da Web do Unified Manager permite verificar se há problemas de conectividade nas configurações do MetroCluster em FC e IP. Descobrir um problema de conectividade cedo permite que você gerencie suas configurações do MetroCluster com eficiência.

### Comportamento do volume durante o switchover e o switchback

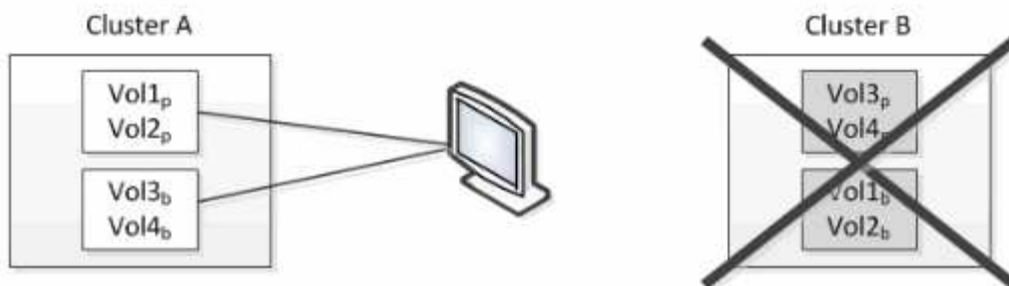
Os eventos que acionam um switchover ou switchback fazem com que os volumes ativos sejam movidos de um cluster para o outro cluster no grupo de recuperação de desastres. Os volumes no cluster que estavam ativos e fornecendo dados aos clientes são interrompidos, e os volumes no outro cluster são ativados e começam a fornecer dados. O Unified Manager monitora apenas os volumes ativos e em execução.

Como os volumes são movidos de um cluster para outro, é recomendável que você monitore os dois clusters. Uma única instância do Unified Manager pode monitorar ambos os clusters em uma configuração do MetroCluster, mas às vezes a distância entre os dois locais exige o uso de duas instâncias do Unified Manager para monitorar ambos os clusters. A figura a seguir mostra uma única instância do Unified Manager:

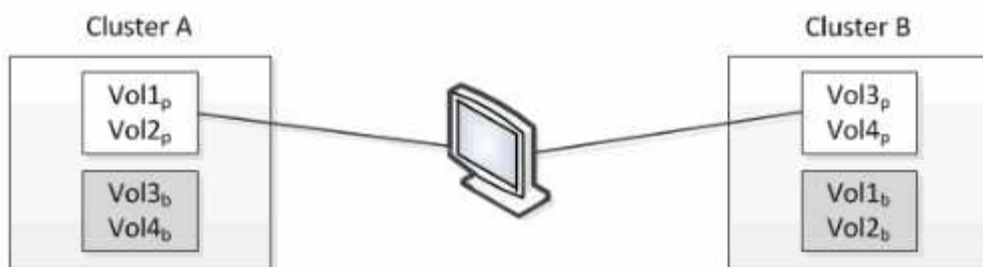
### Normal operation



### Cluster B fails --- switchover to Cluster A



### Cluster B is repaired --- switchback to Cluster B



□ = active and monitored

■ = inactive and not monitored

Os volumes com p em seus nomes indicam os volumes primários, e os volumes com b em seus nomes são volumes de backup espelhados criados pelo SnapMirror.

Durante o funcionamento normal:

- O cluster A tem dois volumes ativos: Vol1<sub>p</sub> e Vol2<sub>p</sub>.
- O cluster B tem dois volumes ativos: Vol3<sub>p</sub> e Vol4<sub>p</sub>.
- O cluster A tem dois volumes inativos: Vol3<sub>b</sub> e Vol4<sub>b</sub>.
- O cluster B tem dois volumes inativos: Vol1<sub>b</sub> e Vol2<sub>b</sub>.

As informações referentes a cada um dos volumes ativos (estatísticas, eventos etc.) são coletadas pelo Unified Manager. As estatísticas Vol1<sub>p</sub> e Vol2<sub>p</sub> são coletadas pelo Cluster A e as estatísticas Vol3<sub>p</sub> e Vol4<sub>p</sub> são coletadas pelo Cluster B.

Após uma falha catastrófica, causa um switchover de volumes ativos do cluster B para o cluster A:

- O cluster A tem quatro volumes ativos: Vol1<sub>p</sub>, Vol2<sub>p</sub>, Vol3<sub>b</sub> e Vol4<sub>b</sub>.



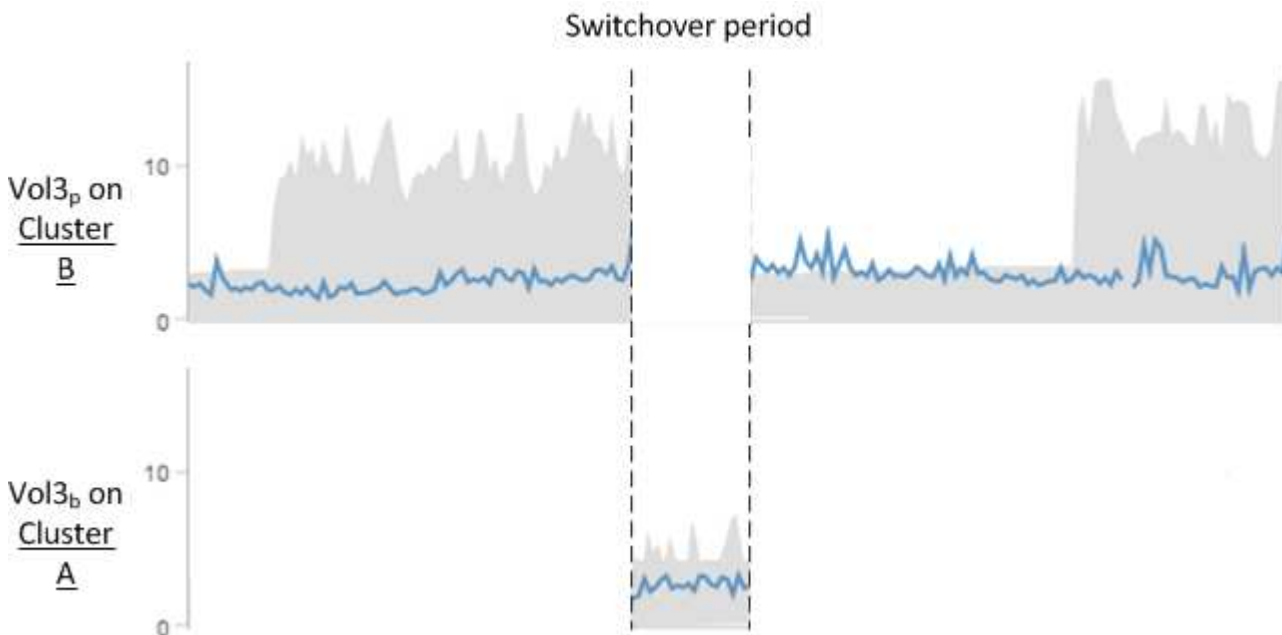
- O cluster B tem quatro volumes inativos: Vol3p, Vol4p, Vol1b e Vol2b.

Como durante a operação normal, as informações referentes a cada um dos volumes ativos são coletadas pelo Unified Manager. Mas neste caso, as estatísticas Vol1p e Vol2p são coletadas pelo Cluster A, e as estatísticas Vol3b e Vol4b também são coletadas pelo Cluster A.

Observe que Vol3p e Vol3b não são os mesmos volumes, porque estão em clusters diferentes. As informações do Unified Manager para Vol3p não são as mesmas que Vol3b:

- Durante o switchover para o cluster A, as estatísticas e os eventos do Vol3p não são visíveis.
- Na primeira mudança, Vol3b parece um novo volume sem informações históricas.

Quando o cluster B é reparado e um switchback é executado, o Vol3p é novamente ativo no cluster B, com as estatísticas históricas e uma lacuna de estatísticas para o período durante o switchover. O Vol3b não pode ser visualizado a partir do cluster A até que ocorra outro switchover:



- Os volumes MetroCluster que estão inativos, por exemplo, Vol3b no cluster A após o switchback, são identificados com a mensagem ""este volume foi excluído"". O volume não é realmente excluído, mas não está sendo monitorado pelo Unified Manager, porque não é o volume ativo.
- Se um único Gerenciador unificado estiver monitorando ambos os clusters em uma configuração do MetroCluster, a pesquisa de volume retornará informações sobre o volume que estiver ativo naquele momento. Por exemplo, uma pesquisa por "Vol3" retornaria estatísticas e eventos para Vol3b no Cluster A se um switchover tiver ocorrido e Vol3 se tornar ativo no Cluster A.




## Definições de status de conectividade de cluster para configuração MetroCluster em FC



A conectividade entre os clusters em uma configuração de MetroCluster em FC pode ser um dos seguintes status: Ideal, impactado ou inativo. Compreender os Estados de conectividade permite-lhe gerir eficazmente as suas configurações do MetroCluster.

Estado da conectividade	Descrição	Ícone apresentado
Ideal	A conectividade entre os clusters na configuração do MetroCluster é normal.	
Impactado	Um ou mais erros comprometem o status da disponibilidade de failover. No entanto, os dois clusters na configuração MetroCluster ainda estão ativos. Por exemplo, quando o link ISL está inativo, quando o link IP entre clusters está inativo ou quando o cluster de parceiros não está acessível.	
Para baixo	A conectividade entre os clusters na configuração do MetroCluster está inativa porque um ou ambos os clusters estão inativos ou os clusters estão no modo failover. Por exemplo, quando o cluster de parceiros está inativo por causa de um desastre ou quando há um switchover planejado para fins de teste.	Switchover com erros:  Comutação bem-sucedida: 

## Definições de status de espelhamento de dados para MetroCluster em FC

As configurações MetroCluster em FC fornecem espelhamento de dados e a capacidade adicional de iniciar um failover se um local inteiro ficar indisponível. O status do espelhamento de dados entre os clusters em uma configuração MetroCluster em FC pode ser normal ou Espelhamento indisponível. A compreensão do status permite que você gerencie suas configurações do MetroCluster com eficiência.

Status do espelhamento de dados	Descrição	Ícone apresentado
Normal	O espelhamento de dados entre os clusters na configuração MetroCluster é normal.	

Status do espelhamento de dados	Descrição	Ícone apresentado
Espelhamento indisponível	O espelhamento de dados entre os clusters na configuração MetroCluster não está disponível devido ao switchover. Por exemplo, quando o cluster de parceiros está inativo por causa de um desastre ou quando há um switchover planejado para fins de teste.	Switchover com erros:  Comutação bem-sucedida: 

## Monitoramento de configurações do MetroCluster

Você pode monitorar problemas de conectividade na configuração do MetroCluster. Os detalhes incluem o status dos componentes e a conectividade em um cluster e o status de conectividade entre os clusters na configuração do MetroCluster. Aqui, você saberá como monitorar problemas de conectividade em clusters protegidos por MetroCluster em configurações FC e MetroCluster em IP.

Você pode monitorar as configurações do MetroCluster a partir das exibições a seguir no painel de navegação esquerdo do Active IQ Unified Manager:

- **Armazenamento > clusters > proteção: Vista MetroCluster**
- **Proteção > relacionamentos > relacionamento: Vista MetroCluster**

O Unified Manager usa alertas de integridade do sistema para indicar o status dos componentes e da conectividade na configuração do MetroCluster.

### Antes de começar

- Os clusters local e remoto em uma configuração do MetroCluster devem ser adicionados ao Active IQ Unified Manager.
- Em uma configuração MetroCluster sobre IP, se um Mediador for suportado, o Mediador deve ser configurado e adicionado ao cluster pela API correspondente.
- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

## Monitore problemas de conectividade no MetroCluster com a configuração de FC

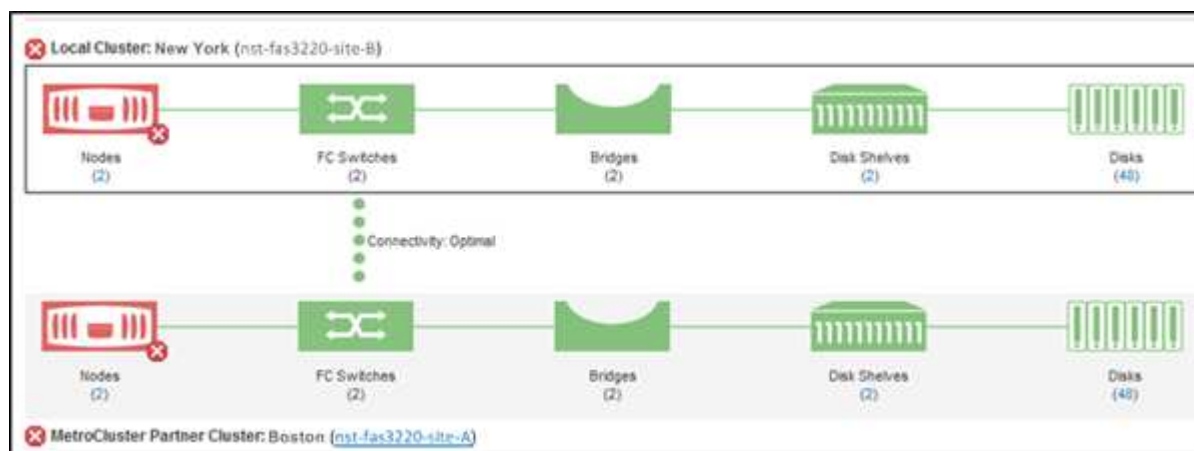
Para clusters em uma configuração MetroCluster sobre FC, os gráficos de conectividade são exibidos na página de detalhes **Cluster / Health**. Siga estes passos.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > clusters**.

É apresentada uma lista de todos os clusters monitorizados.

2. Na exibição **proteção: MetroCluster**, clique no nome do cluster para o qual deseja exibir os detalhes de configuração do MetroCluster sobre FC. Como alternativa, você pode filtrar por clusters em uma configuração do MetroCluster.
3. Na página de detalhes **Cluster / Health**, clique na guia **conetividade MetroCluster**. A guia **conetividade MetroCluster** está disponível apenas para configurações MetroCluster em FC.



A topologia da configuração do MetroCluster é exibida na área de objeto do cluster correspondente. Pode utilizar as informações apresentadas na página Cluster / Health details (Detalhes do Cluster/Health) para corrigir quaisquer problemas de conectividade. Por exemplo, se a conectividade entre o nó e o switch em um cluster estiver inativa, o seguinte ícone é exibido:



Se mover o ponteiro sobre o ícone, poderá visualizar informações detalhadas sobre o evento gerado.

Se você descobrir problemas de conectividade na configuração do MetroCluster, faça login no Gerenciador de sistema ou acesse a CLI do ONTAP para resolver os problemas.

Para obter mais informações sobre como determinar a integridade do cluster, "[Determinando a integridade do cluster na configuração de MetroCluster em FC](#)" consulte .

### Monitore problemas de conectividade na configuração MetroCluster sobre IP

Para clusters em uma configuração MetroCluster sobre IP, os gráficos de conectividade são exibidos na página **clusters**. Siga estes passos.

#### Passos

1. No painel de navegação esquerdo, clique em **Storage > clusters**.

É apresentada uma lista de todos os clusters monitorizados.

2. Na exibição **proteção: Metroclusters**, clique no nome do cluster para o qual você deseja exibir os detalhes de configuração do MetroCluster sobre IP. Como alternativa, você pode filtrar por clusters em uma configuração do MetroCluster.
3. Expanda a linha clicando no ícone de cuidado ▾. O ícone de cuidado aparece apenas para um cluster protegido pela configuração MetroCluster sobre IP.

Você pode visualizar a topologia dos locais de origem e espelho, bem como o Mediador, se houver, usado para a conexão. Você pode exibir as seguintes informações:

- Conetividade entre os sites
- Problemas de saúde e disponibilidade, se houver, em ambos os sites
- Questões relacionadas com o mediador
- Problemas relacionados à replicação.



São comunicados os seguintes Estados: Crítico (❌), erro (⚠️) ou normal (✅). Você também pode visualizar o status de replicação de dados agregados dos dados primários e espelhados na mesma topologia.

No diagrama a seguir, você pode ver que a conetividade entre os clusters de origem e destino não está disponível e o Mediador entre eles não está configurado.



4. Clique no ícone de estado. É apresentada uma mensagem com a definição de erro. Se um evento tiver sido gerado para o problema na configuração do MetroCluster sobre IP, você pode clicar no botão **Exibir evento** na mensagem e exibir os detalhes do evento. Quando você resolver o problema e o evento, o ícone de status dessa topologia mudará para normal (✅).
5. Você pode ver mais detalhes de configuração nas seções **Visão geral do MetroCluster** e **proteção** na guia **Configuração** da página de detalhes **Cluster / Saúde**.



Somente para uma configuração MetroCluster sobre IP, você pode ter a visualização da topologia do cluster na página **clusters**. Para clusters em uma configuração MetroCluster sobre FC, a topologia é exibida na guia **conetividade MetroCluster** na página de detalhes **Cluster / Saúde**.

### Informações relacionadas

- ["Página de detalhes de cluster / Saúde"](#)
- Para obter informações sobre a visualização **relação:MetroCluster**, ["Monitoramento de configurações do MetroCluster"](#) consulte .
- Para obter informações sobre a 1 visualização **relação: Status de transferência do último mês**, ["Relação: Último 1 mês visualização do Status da transferência"](#) consulte .
- Para obter informações sobre a 1 visualização **relação: Taxa de transferência do último mês**, ["Relação:](#)

[Último 1 mês visualização da taxa de transferência](#) consulte .

- Para obter informações sobre a visualização **relacionamento: Todas as relações**, "[Relacionamento: Todos os relacionamentos são exibidos](#)" consulte .

## Monitoramento da replicação do MetroCluster

Você pode monitorar e diagnosticar a condição geral de integridade das conexões lógicas enquanto espelha os dados. Você pode identificar os problemas ou qualquer risco que interrompe o espelhamento de componentes de cluster, como agregados, nós e máquinas virtuais de storage.

O Unified Manager usa alertas de integridade do sistema para monitorar o status dos componentes e a conectividade na configuração do MetroCluster.

### Antes de começar

O cluster local e remoto na configuração do MetroCluster deve ser adicionado ao Unified Manager

### Visualização da replicação para configurações MetroCluster sobre IP

Para configurações MetroCluster sobre IP, o status da replicação de dados é exibido na exibição de peek de topologia de um cluster protegido pelo MetroCluster sobre IP a partir das seguintes exibições no painel de navegação esquerdo do Unified Manager:

- **Armazenamento > clusters > proteção: Vista MetroCluster**
- **Proteção > relacionamentos > relacionamento: Vista MetroCluster**

Para obter informações, "[Monitore problemas de conectividade no MetroCluster sobre IP](#)" consulte .

### Visualização da replicação para MetroCluster em configurações de FC

Siga estas etapas para determinar quaisquer problemas na replicação de dados para a configuração MetroCluster em FC.

#### Passos

1. No painel de navegação esquerdo, clique em **Storage > clusters**.

É apresentada uma lista dos clusters monitorizados.

2. Na exibição **Saúde: Todos os clusters**, clique no nome do cluster para o qual deseja exibir os detalhes da replicação do MetroCluster. Na página **Cluster / Health details**, clique na guia **MetroCluster Replication**.

A topologia da configuração do MetroCluster a ser replicada é exibida no local local na área de objeto do cluster correspondente com as informações sobre o local remoto onde os dados estão sendo espelhados. Se mover o ponteiro sobre o ícone, poderá visualizar informações detalhadas sobre o evento gerado.

Pode utilizar as informações apresentadas na página Cluster / Health details (Detalhes do Cluster/Health) para corrigir quaisquer problemas de replicação. Se você descobrir problemas de espelhamento na configuração do MetroCluster, faça login no Gerenciador de sistema ou acesse a CLI do ONTAP para resolver os problemas.

### Informações relacionadas

## Gerenciamento de cotas

Você pode usar cotas de usuário e grupo para limitar a quantidade de espaço em disco ou o número de arquivos que um usuário ou um grupo de usuários podem usar. Você pode exibir informações de cota de usuário e grupo de usuários, como o uso de disco e arquivo e os vários limites definidos nos discos.

### Quais são os limites de cota

Limites de cota de usuário são valores que o servidor do Unified Manager usa para avaliar se o consumo de espaço por um usuário está se aproximando do limite ou atingiu o limite definido pela cota do usuário. Se o limite de software for cruzado ou se o limite rígido for atingido, o servidor do Unified Manager gera eventos de cota de usuário.

Por padrão, o servidor do Unified Manager envia um e-mail de notificação aos usuários que cruzaram o limite de cota ou atingiram o limite rígido da cota e para os quais eventos de cota de usuário estão configurados. Os usuários com a função Administrador do aplicativo podem configurar alertas que notificam os destinatários especificados dos eventos de cota de usuário ou grupo de usuários.

Você pode especificar limites de cota usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

### Exibindo cotas de usuário e grupo de usuários

A página de detalhes de VM/integridade de storage exibe informações sobre as cotas de usuário e grupo de usuários configuradas no SVM. Você pode exibir o nome do usuário ou grupo de usuários, os limites definidos nos discos e arquivos, o espaço usado em disco e arquivo e o endereço de e-mail para notificação.

#### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

#### Passos

1. No painel de navegação esquerdo, clique em **Storage > Storage VMs**.
2. Na exibição **Saúde: Todas as VMs de armazenamento**, selecione uma VM de armazenamento e clique na guia **cotas de usuário e grupo**.

#### Informações relacionadas

["Adicionando usuários"](#)

### Criando regras para gerar endereços de e-mail

Você pode criar regras para especificar o endereço de e-mail com base na cota de usuário associada a clusters, máquinas virtuais de armazenamento (SVMs), volumes, qtrees, usuários ou grupos de usuários. Uma notificação é enviada para o endereço de e-mail especificado quando há uma violação de cota.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter revisado as diretrizes na página regras para gerar Endereço de e-mail de cota de usuário e grupo.

Você deve definir as regras para endereços de e-mail de cota e inseri-los na ordem em que deseja executá-los. Por exemplo, se você quiser usar o endereço de e-mail [abc@xyz.com](mailto:abc@xyz.com) para receber notificações sobre violações de cota para abc e usar o endereço de e-mail para todos os outros grupos, as regras devem ser listadas na seguinte ordem:

- Se ("abc") o [abc@xyz.com](mailto:abc@xyz.com)
- Se (

Se nenhum dos critérios para as regras especificadas for atendido, a regra padrão será usada:

SE ("USER\_OR\_GROUP" \* ), ENTÃO O DOMÍNIO "USER\_OR\_GROUP"

### Passos

1. No painel de navegação esquerdo, clique em **Geral > regras de e-mail de cota**.
2. Introduza a regra com base nos seus critérios.
3. Clique em **Validar** para validar a sintaxe da regra.

Uma mensagem de erro é exibida se a sintaxe da regra estiver incorreta. Você deve corrigir a sintaxe e clicar em **Validar** novamente.

4. Clique em **Salvar**.
5. Verifique se o endereço de e-mail que você criou é exibido na guia **cotas de usuário e grupo** da página de detalhes Storage **VM / Health**.

## Criando um formato de notificação por e-mail para cotas de usuários e grupos de usuários

Você pode criar um formato de notificação para os e-mails que são enviados para um usuário ou um grupo de usuários quando houver um problema relacionado à cota (limite de software violado ou limite rígido atingido).

### Antes de começar

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

### Passos

1. No painel de navegação à esquerda, clique em **Geral > formato de e-mail da cota**.
2. Insira ou modifique os detalhes nos campos **de**, **Assunto** e **Detalhes do e-mail**.
3. Clique em **Preview** para visualizar a notificação por e-mail.
4. Clique em **Fechar** para fechar a janela de visualização.
5. Modifique o conteúdo da notificação por e-mail, se necessário.
6. Clique em **Salvar**.



## Editando endereços de e-mail de cota de usuário e grupo

É possível modificar os endereços de e-mail com base na cota de usuário associada a clusters, máquinas virtuais de armazenamento (SVMs), volumes, qtrees, usuários ou grupos de usuários. Você pode modificar o endereço de e-mail quando quiser substituir o endereço de e-mail gerado pelas regras especificadas na caixa de diálogo regras para gerar Endereço de e-mail de cota de usuário e grupo.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Tem de ter revisto a ["diretrizes para a criação de regras"](#).

Se você editar um endereço de e-mail, as regras para gerar os endereços de e-mail de cota de usuário e grupo não serão mais aplicáveis à cota. Para que as notificações sejam enviadas para o endereço de e-mail gerado pelas regras especificadas, você deve excluir o endereço de e-mail e salvar a alteração.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > SVMs**.
2. Na exibição **Saúde: Todas as VMs de armazenamento**, selecione um SVM e clique na guia **cotas de usuário e grupo**.
3. Clique em **Editar endereço de e-mail** abaixo da linha de guias.
4. Na caixa de diálogo **Editar endereço de e-mail**, execute a ação apropriada:

Se...	Então...
Você deseja que as notificações sejam enviadas para o endereço de e-mail gerado pelas regras especificadas	<ol style="list-style-type: none"><li>a. Exclua o endereço de e-mail no campo <b>Endereço de e-mail</b>.</li><li>b. Clique em <b>Salvar</b>.</li><li>c. Atualize o navegador pressionando F5 para recarregar a caixa de diálogo Editar endereço de e-mail. O endereço de e-mail gerado pela regra especificada é exibido no campo <b>Endereço de e-mail</b>.</li></ol>
Você deseja que as notificações sejam enviadas para um endereço de e-mail especificado	<ol style="list-style-type: none"><li>a. Modifique o endereço de e-mail no campo <b>Endereço de e-mail</b>.</li><li>b. Clique em <b>Salvar</b>. As regras para gerar os endereços de e-mail de cota de usuário e grupo não são mais aplicáveis à cota.</li></ol>

## Compreender mais sobre quotas

Entender os conceitos sobre cotas ajuda você a gerenciar suas cotas de usuário e cotas de grupo de usuários de forma eficiente.

## Visão geral do processo de cota

As quotas podem ser suaves ou difíceis. As cotas flexíveis fazem com que o ONTAP envie uma notificação quando os limites especificados forem excedidos e as cotas rígidas impedem que uma operação de gravação seja bem-sucedida quando os limites especificados forem excedidos.

Quando o ONTAP recebe uma solicitação de um usuário ou grupo de usuários para gravar em um FlexVol volume, ele verifica se as cotas estão ativadas nesse volume para o usuário ou grupo de usuários e determina o seguinte:

- Se o limite rígido será atingido

Se sim, a operação de gravação falha quando o limite rígido é atingido e a notificação de cota rígida é enviada.

- Se o limite flexível será violado

Se sim, a operação de gravação é bem-sucedida quando o limite de software é violado e a notificação de cota de software é enviada.

- Se uma operação de gravação não excederá o limite de software

Se sim, a operação de gravação é bem-sucedida e nenhuma notificação é enviada.

## Sobre cotas

As cotas fornecem uma maneira de restringir ou rastrear o espaço em disco e o número de arquivos usados por um usuário, grupo ou qtree. Você especifica cotas usando o `/etc/quotas` arquivo. As cotas são aplicadas a um volume ou qtree específico.

## Por que você usa cotas

Você pode usar cotas para limitar o uso de recursos em volumes do FlexVol, fornecer notificações quando o uso de recursos atingir níveis específicos ou controlar o uso dos recursos.

Você especifica uma cota pelos seguintes motivos:

- Para limitar a quantidade de espaço em disco ou o número de arquivos que podem ser usados por um usuário ou grupo, ou que podem ser contidos por uma qtree
- Para rastrear a quantidade de espaço em disco ou o número de arquivos usados por um usuário, grupo ou qtree, sem impor um limite
- Avisar os usuários quando o uso do disco ou o uso do arquivo for alto

## Descrição das caixas de diálogo cotas

Você pode usar a opção apropriada na guia cotas de usuário e grupo na exibição integridade: Todas as VMs de armazenamento para configurar o formato da notificação de e-mail enviada quando ocorre um problema relacionado à cota e configurar regras

para especificar endereços de e-mail com base na cota de usuário.

### **Página formato de notificação por e-mail**

A página formato de notificação por e-mail exibe as regras do e-mail que é enviado para um usuário ou grupo de usuários quando há um problema relacionado à cota (limite de software violado ou limite rígido atingido).

A notificação por e-mail é enviada somente quando os seguintes eventos de cota de usuário ou grupo são gerados: Limite de espaço em disco de cota de usuário ou grupo violado, limite de espaço em disco de cota de usuário ou grupo violado, limite de espaço em disco de cota de usuário ou de grupo atingido.

- **De**

Exibe o endereço de e-mail a partir do qual o e-mail é enviado, que você pode modificar. Por padrão, este é o endereço de e-mail especificado na página notificações.

- **Assunto**

Exibe o assunto do e-mail de notificação.

- **Detalhes do e-mail**

Exibe o texto do e-mail de notificação. Você pode modificar o texto com base em suas necessidades. Por exemplo, você pode fornecer informações relacionadas aos atributos de cota e reduzir o número de palavras-chave. No entanto, você não deve modificar as palavras-chave.

Palavras-chave válidas são as seguintes:

- **NOME\_DO\_EVENTO**

Especifica o nome do evento que causou a notificação por e-mail.

- **QUOTA\_ALVO**

Especifica a qtree ou volume em que a cota é aplicável.

- **QUOTA\_USED\_PERCENT**

Especifica a porcentagem de limite de disco rígido, limite de disco rígido, limite de arquivo ou limite de software de arquivo que é usado pelo usuário ou grupo de usuários.

- **QUOTA\_LIMITE**

Especifica o limite rígido do disco ou o limite rígido do arquivo que é alcançado pelo usuário ou grupo de usuários e um dos seguintes eventos é gerado:

- Limite de espaço em disco de quota de utilizador ou de grupo atingido
- Limite de espaço em disco de quota de utilizador ou de grupo atingido
- Limite rígido de contagem de ficheiros de quota de utilizador ou grupo atingido
- Limite de software contagem de ficheiros de quota de utilizador ou grupo atingido

- **QUOTA\_USADA**

Especifica o espaço em disco usado ou o número de arquivos criados pelo usuário ou grupo de usuários.

- QUOTA\_UTILIZADOR

Especifica o nome do usuário ou do grupo de usuários.

### Botões de comando

Os botões de comando permitem visualizar, salvar ou cancelar as alterações feitas no formato de notificação por e-mail:

- **Pré-visualização**

Exibe uma visualização do e-mail de notificação.

- **Restaurar para padrões de fábrica**

Permite restaurar o formato de notificação para os valores padrão de fábrica.

- **Guardar**

Guarda as alterações efetuadas no formato de notificação.

### Regras para gerar a página Endereço de e-mail de cota de usuário e grupo

A página regras para gerar endereço de e-mail de cota de usuário e grupo permite criar regras para especificar endereços de e-mail com base na cota de usuário associada a clusters, SVMs, volumes, qtrees, usuários ou grupos de usuários. Uma notificação é enviada para o endereço de e-mail especificado quando uma cota é violada.

#### Área de regras

Você deve definir as regras para um endereço de e-mail de cota. Você também pode adicionar comentários para explicar as regras.

#### Como você define regras

Você deve inserir as regras na ordem em que deseja executá-las. Se o critério da primeira regra for atendido, o endereço de e-mail será gerado com base nessa regra. Se o critério não for cumprido, então o critério para a próxima regra é considerado, e assim por diante. Cada linha lista uma regra separada. A regra padrão é a última regra da lista. Você pode alterar a ordem de prioridade das regras. No entanto, não é possível alterar a ordem da regra padrão.

Por exemplo, se você quiser usar o endereço de e-mail [qtree1@xyz.com](mailto:qtree1@xyz.com) para receber notificações sobre violações de cota para qtree1 e usar o endereço de e-mail [admin@xyz.com](mailto:admin@xyz.com) para todos os outros qtrees, as regras devem ser listadas na seguinte ordem:

- Se ("QTREE" qtree1), então [qtree1@xyz.com](mailto:qtree1@xyz.com)
- Se ("QTREE" \* ), então [admin@xyz.com](mailto:admin@xyz.com)

Se nenhum dos critérios para as regras especificadas for atendido, a regra padrão será usada:

SE ("USER\_OR\_GROUP" \* ), ENTÃO O DOMÍNIO "USER\_OR\_GROUP"

Se mais de um usuário tiver a mesma cota, os nomes dos usuários serão exibidos como valores separados por vírgula e as regras não serão aplicáveis à cota.

### Como você adiciona comentários

Você pode adicionar comentários para explicar as regras. Você deve usar no início de cada comentário e cada linha lista um comentário separado.

### Sintaxe de regras

A sintaxe da regra deve ser uma das seguintes:

- `se ( valid variableoperator * ), então email ID@domain name`

`se` é uma palavra-chave e está em minúsculas. O operador é `*`. O ID de e-mail pode conter qualquer caractere, as variáveis válidas `user_or_group`, `USER` ou `GROUP`, ou uma combinação de qualquer caractere e as variáveis válidas `user_or_group`, `USER` ou `GROUP`. O nome de domínio pode conter qualquer caractere, a variável válida `DOMÍNIO` ou uma combinação de qualquer caractere e a variável válida `DOMÍNIO`. As variáveis válidas podem estar em maiúsculas ou minúsculas, mas não devem ser uma combinação de ambas. Por exemplo, `o domínio` e `o DOMÍNIO` são válidos, mas `o domínio` não é uma variável válida.

- `se ( valid variableoperator `string` ), então email ID@domain name`

`se` é uma palavra-chave e é minúscula. O operador pode conter `ou` ou `O`. O ID de e-mail pode conter qualquer caractere, as variáveis válidas `user_or_group`, `USER` ou `GROUP`, ou uma combinação de qualquer caractere e as variáveis válidas `user_or_group`, `USER` ou `GROUP`. O nome de domínio pode conter qualquer caractere, a variável válida `DOMÍNIO` ou uma combinação de qualquer caractere e a variável válida `DOMÍNIO`. As variáveis válidas podem estar em maiúsculas ou minúsculas, mas não devem ser uma combinação de ambas. Por exemplo, `o domínio` e `o DOMÍNIO` são válidos, mas `o domínio` não é uma variável válida.

### Botões de comando

Os botões de comando permitem salvar, validar ou cancelar as regras criadas:

- **Validar**

Valida a sintaxe da regra criada. Se houver erros durante a validação, a regra que gera o erro é exibida juntamente com uma mensagem de erro.

- **Restaurar para padrões de fábrica**

Permite restaurar as regras de endereço para os valores padrão de fábrica.

- **Guardar**

Valida a sintaxe da regra e salva a regra se não houver erros. Se houver erros durante a validação, a regra que gera o erro é exibida juntamente com uma mensagem de erro.

# Solução de problemas

As informações de solução de problemas ajudam a identificar e resolver problemas que você encontra ao usar o Unified Manager.

## Adicionando espaço em disco ao diretório do banco de dados do Unified Manager

O diretório do banco de dados do Unified Manager contém todos os dados de integridade e desempenho coletados dos sistemas ONTAP. Algumas circunstâncias podem exigir que você aumente o tamanho do diretório do banco de dados.

Por exemplo, o diretório do banco de dados pode ficar cheio se o Unified Manager estiver coletando dados de um grande número de clusters onde cada cluster tem muitos nós. Você receberá um evento de aviso quando o diretório do banco de dados estiver 90% cheio e um evento crítico quando o diretório estiver 95% cheio.



Nenhum dado adicional é coletado de clusters depois que o diretório atinge 95% cheio.

As etapas necessárias para adicionar capacidade ao diretório de dados são diferentes dependendo se o Unified Manager está sendo executado em um servidor VMware ESXi, em um servidor Red Hat Linux ou em um servidor Microsoft Windows.

## Adicionando espaço ao disco de dados da máquina virtual VMware

Se você precisar aumentar a quantidade de espaço no disco de dados para o banco de dados do Unified Manager, poderá adicionar capacidade após a instalação aumentando o espaço em disco usando o console de manutenção do Unified Manager.

### Antes de começar

- Você deve ter acesso ao vSphere Client.
- A máquina virtual não deve ter instantâneos armazenados localmente.
- Tem de ter as credenciais do utilizador de manutenção.

Recomendamos que você faça backup de sua máquina virtual antes de aumentar o tamanho dos discos virtuais.

### Passos

1. No cliente vSphere, selecione a máquina virtual do Unified Manager e adicione mais capacidade de disco aos dados `disk` 3. Consulte a documentação da VMware para obter detalhes.

Em alguns casos raros, a implantação do Unified Manager usa "disco rígido 2" para o disco de dados em vez de "disco rígido 3". Se isso tiver ocorrido em sua implantação, aumente o espaço de qualquer disco maior. O disco de dados sempre terá mais espaço do que o outro disco.

2. No cliente vSphere, selecione a máquina virtual do Unified Manager e, em seguida, selecione a guia **Console**.
3. Clique na janela do console e, em seguida, faça login no console de manutenção usando seu nome de usuário e senha.
4. No **Menu Principal**, insira o número da opção **Configuração do sistema**.
5. No **Menu de Configuração do sistema**, insira o número da opção **aumentar o tamanho do disco de**

**dados.**

## Adicionando espaço ao diretório de dados do host Linux

Se você atribuiu espaço em disco insuficiente ao `/opt/netapp/data` diretório para oferecer suporte ao Unified Manager quando configurou originalmente o host Linux e instalou o Unified Manager, você poderá adicionar espaço em disco após a instalação aumentando o espaço em disco `/opt/netapp/data` no diretório.

### Antes de começar

Você deve ter acesso de usuário raiz à máquina Red Hat Enterprise Linux na qual o Unified Manager está instalado.

Recomendamos que você faça backup do banco de dados do Unified Manager antes de aumentar o tamanho do diretório de dados.

### Passos

1. Faça login como usuário root na máquina Linux na qual você deseja adicionar espaço em disco.
2. Pare o serviço Unified Manager e o software MySQL associado na ordem mostrada: `systemctl stop ocieau ocie mysqld`
3. Crie uma pasta de backup temporária (por exemplo, `/backup-data`) com espaço em disco suficiente para conter os dados no diretório atual `/opt/netapp/data`.
4. Copie o conteúdo e a configuração de privilégios do diretório existente `/opt/netapp/data` para o diretório de dados de backup:

```
cp -arp /opt/netapp/data/* /backup-data
```

5. Se o se Linux estiver ativado:

- a. Obtenha o tipo se Linux para pastas na pasta existente `/opt/netapp/data`:

```
se_type=`ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1
```

O sistema retorna uma confirmação semelhante à seguinte:

```
echo $se_type  
mysqld_db_t
```

- a. Execute o `chcon` comando para definir o tipo se Linux para o diretório de backup:

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Remova o conteúdo do `/opt/netapp/data` diretório:

- a. `cd /opt/netapp/data`

- b. `rm -rf *`

7. Expanda o tamanho `/opt/netapp/data` do diretório para um mínimo de 150 GB por meio de comandos

LVM ou adicionando discos extras.



Se você criou `/opt/netapp/data` a partir de um disco, então você não deve tentar montar `/opt/netapp/data` como um compartilhamento NFS ou CIFS. Porque, neste caso, se você tentar expandir o espaço em disco, alguns comandos LVM, `resize` como e `extend` podem não funcionar como esperado.

8. Confirme que o `/opt/netapp/data` proprietário do diretório (`mysql`) e o grupo (`root`) estão inalterados:

```
ls -ltr /opt/netapp/ | grep data
```

O sistema retorna uma confirmação semelhante à seguinte:

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. Se o `se Linux` estiver ativado, confirme que o contexto `/opt/netapp/data` do diretório ainda está definido como `mysqld_db_t`:

a. `touch /opt/netapp/data/abc`

b. `ls -Z /opt/netapp/data/abc`

O sistema retorna uma confirmação semelhante à seguinte:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0  
/opt/netapp/data/abc
```

10. Exclua o arquivo `abc` para que esse arquivo estranho não cause um erro de banco de dados no futuro.

11. Copie o conteúdo `backup-data` de volta para o diretório expandido `/opt/netapp/data`:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Se o `se Linux` estiver ativado, execute o seguinte comando:

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. Inicie o serviço MySQL:

```
systemctl start mysqld
```

14. Após o início do serviço MySQL, inicie os serviços `ocie` e `ocieau` na ordem mostrada:

```
systemctl start ocie ocieau
```

15. Depois de todos os serviços serem iniciados, exclua a pasta de `/backup-data` backup :

```
rm -rf /backup-data
```



## Adicionando espaço à unidade lógica do servidor Microsoft Windows

Se você precisar aumentar a quantidade de espaço em disco para o banco de dados do Unified Manager, poderá adicionar capacidade à unidade lógica na qual o Unified Manager está instalado.

### Antes de começar

Você deve ter o Privileges administrador do Windows.

Recomendamos que você faça backup do banco de dados do Unified Manager antes de adicionar espaço em disco.

### Passos

1. Inicie sessão como administrador no servidor Windows no qual pretende adicionar espaço em disco.
2. Siga a etapa que corresponde ao método que você deseja usar para adicionar mais espaço:

Opção	Descrição
Em um servidor físico, adicione capacidade à unidade lógica na qual o servidor do Unified Manager está instalado.	Siga as etapas no tópico da Microsoft: <a href="#">"Estender um volume básico"</a>
Em um servidor físico, adicione uma unidade de disco rígido.	Siga as etapas no tópico da Microsoft: <a href="#">"Adicionar unidades de disco rígido"</a>
Em uma máquina virtual, aumente o tamanho de uma partição de disco.	Siga as etapas no tópico VMware: <a href="#">"Aumentando o tamanho de uma partição de disco"</a>

## Alterar o intervalo de coleta de estatísticas de desempenho

O intervalo de coleta padrão para estatísticas de desempenho é de 5 minutos. Você pode alterar esse intervalo para 10 ou 15 minutos se achar que coleções de clusters grandes não estão finalizadas dentro do tempo padrão. Essa configuração afeta a coleção de estatísticas de todos os clusters que essa instância do Unified Manager está monitorando.

### Antes de começar

Você deve ter uma ID de usuário e senha autorizados para fazer login no console de manutenção do servidor do Unified Manager.

A questão das coleções de estatísticas de desempenho que não estão terminando no tempo é indicada pelas mensagens de banner `Unable to consistently collect from cluster <cluster_name>` or `Data collection is taking too long on cluster <cluster_name>`.

Você deve alterar o intervalo de coleta somente quando necessário devido a um problema de coleta de estatísticas. Não altere esta definição por qualquer outro motivo.



Alterar esse valor da configuração padrão de 5 minutos pode afetar o número e a frequência dos eventos de desempenho reportados pelo Unified Manager. Por exemplo, os limites de desempenho definidos pelo sistema acionam eventos quando a política é excedida por 30 minutos. Ao usar coleções de 5 minutos, a política deve ser excedida por seis coleções consecutivas. Para coleções de 15 minutos, a política deve ser excedida por apenas dois períodos de coleta.

Uma mensagem na parte inferior da página Configuração do cluster indica o intervalo de coleta de dados estatísticos atual.

### Passos

1. Faça login usando SSH como o usuário de manutenção no host do Unified Manager.

Os prompts do console do Unified Manager maintenance são exibidos.

2. Digite o número da opção de menu chamada **Configuração do intervalo de polling de desempenho** e pressione Enter.
3. Se solicitado, digite a senha do usuário de manutenção novamente.
4. Digite o número do novo intervalo de polling que deseja definir e pressione Enter.

Se você alterou o intervalo de coleta do Unified Manager para 10 ou 15 minutos e tiver uma conexão atual com um provedor de dados externo (como Graphite), altere o intervalo de transmissão do provedor de dados para que ele seja igual ou maior que o intervalo de coleta do Unified Manager.

## Alterar a duração do tempo em que o Unified Manager retém os dados de eventos e performance

Por padrão, o Unified Manager armazena dados de eventos e dados de performance por 6 meses para todos os clusters monitorados. Após esse tempo, os dados mais antigos são excluídos automaticamente para dar espaço para novos dados. Esse período de tempo padrão funciona bem para a maioria das configurações, mas configurações muito grandes, com muitos clusters e nós, podem precisar reduzir o período de retenção para que o Unified Manager funcione de forma otimizada.

### Antes de começar

Tem de ter a função Administrador de aplicações.

Você pode alterar os períodos de retenção desses dois tipos de dados na página retenção de dados. Essas configurações afetam a retenção de dados de todos os clusters que essa instância do Unified Manager está monitorando.



O Unified Manager coleta estatísticas de performance a cada 5 minutos. Todos os dias, as estatísticas de 5 minutos são resumidas em estatísticas de desempenho por hora. Ele retém 30 dias de dados de performance histórica de 5 minutos e 6 meses de dados de performance resumidos por hora (por padrão).

Você deve reduzir o período de retenção somente se estiver sem espaço ou se o backup e outras operações estiverem demorando muito tempo para serem concluídas. Reduzir o período de retenção tem os seguintes efeitos:

- Os dados de desempenho antigos são excluídos do banco de dados do Unified Manager após a meia-noite.
- Os dados de eventos antigos são excluídos imediatamente do banco de dados do Unified Manager.
- Os eventos anteriores ao período de retenção deixarão de estar disponíveis para visualização na interface do utilizador.
- Os locais na IU onde as estatísticas de desempenho por hora são exibidas ficarão em branco antes do período de retenção.
- Se o período de retenção de eventos exceder o período de retenção de dados de desempenho, uma mensagem será exibida sob o controle deslizante de desempenho, avisando que eventos de desempenho mais antigos podem não ter dados de backup em seus gráficos associados.

### Passos

1. No painel de navegação esquerdo, clique em **políticas > retenção de dados**.
2. Na página **retenção de dados**, selecione a ferramenta de controle deslizante na área retenção de eventos ou retenção de dados de desempenho e mova-a para o número de meses em que os dados devem ser mantidos e clique em **Salvar**.

### Erro de autenticação desconhecido

Quando você está executando uma operação relacionada à autenticação, como adicionar, editar, excluir ou testar usuários ou grupos remotos, a seguinte mensagem de erro pode ser exibida: `Unknown authentication error`.

### Causa

Esse problema pode ocorrer se você tiver definido um valor incorreto para as seguintes opções:

- Nome do administrador do serviço de autenticação do ativo Directory
- Vincular Nome distinto do serviço de autenticação OpenLDAP

### Ações corretivas

1. No painel de navegação esquerdo, clique em **Geral > Autenticação remota**.
2. Com base no serviço de autenticação que selecionou, introduza as informações adequadas para Nome de administrador ou Nome distinto vincular.
3. Clique em **Test Authentication** para testar a autenticação com os detalhes especificados.
4. Clique em **Salvar**.

### Utilizador não encontrado

Quando você está executando uma operação relacionada à autenticação, como adicionar, editar, excluir ou testar usuários ou grupos remotos, a seguinte mensagem de erro é exibida: `User not found`.

### Causa

Este problema pode ocorrer se o utilizador existir no servidor AD ou no servidor LDAP e se tiver definido o nome distinto base para um valor incorreto.

## Ações corretivas

1. No painel de navegação esquerdo, clique em **Geral > Autenticação remota**.
2. Introduza as informações adequadas para o nome distinto da base.
3. Clique em **Salvar**.

## Problema com a adição de LDAP usando outros serviços de autenticação

Quando você seleciona outros como o serviço de autenticação, o usuário e a classe de objeto do grupo retêm os valores do modelo selecionado anteriormente. Se o servidor LDAP não usar os mesmos valores, a operação pode falhar.

### Causa

Os usuários não estão configurados corretamente no OpenLDAP.

## Ações corretivas

Você pode corrigir manualmente esse problema usando uma das seguintes soluções alternativas.

Se a classe de objeto de usuário LDAP e a classe de objeto de grupo forem usuário e grupo, respectivamente, execute as seguintes etapas:

1. No painel de navegação à esquerda, clique em **Geral > Autenticação remota**.
2. No menu suspenso **Authentication Service**, selecione **active Directory** e, em seguida, selecione **Others**.
3. Preencha os campos de texto.

Se a classe de objeto de usuário LDAP e a classe de objeto de grupo forem posixAccount e posixGroup, respectivamente, execute as seguintes etapas:

1. No painel de navegação à esquerda, clique em **Geral > Autenticação remota**.
2. No menu suspenso **Authentication Service**, selecione **OpenLDAP** e, em seguida, selecione **Others**.
3. Preencha os campos de texto.

Se as duas primeiras soluções alternativas não se aplicarem, chame a `option-set` API e defina `auth.ldap.userObjectClass` as opções e `auth.ldap.groupObjectClass` para os valores corretos.

# Gerenciar eventos e alertas

## Gerenciamento de eventos

Os eventos ajudam a identificar problemas nos clusters monitorados.

### Quais são os eventos da plataforma Active IQ

O Unified Manager pode exibir eventos que foram descobertos pela plataforma Active IQ. Esses eventos são criados executando um conjunto de regras contra as mensagens do AutoSupport geradas a partir de todos os sistemas de storage monitorados pelo Unified Manager.

Para obter mais informações, "[Como os eventos da plataforma Active IQ são gerados](#)" consulte .

O Unified Manager verifica automaticamente um novo arquivo de regras e somente baixa um novo arquivo quando há regras mais recentes. Em sites sem acesso à rede externa, você precisa fazer o upload das regras manualmente de **Gerenciamento de armazenamento > Configuração do evento > regras de upload**.

Esses eventos do Active IQ não se sobrepõem aos eventos existentes do Unified Manager e identificam incidentes ou riscos relacionados a problemas de configuração do sistema, cabeamento, práticas recomendadas e disponibilidade.

Para obter mais informações sobre como ativar eventos de plataforma, "[Ativar eventos do portal Active IQ](#)" consulte . Para obter mais informações sobre como carregar o arquivo de regras, "[Carregar um novo arquivo de regras do Active IQ](#)" consulte .

O NetApp Active IQ é um serviço baseado em nuvem que fornece análises preditivas e suporte proativo para otimizar as operações do sistema de storage na nuvem híbrida da NetApp. Consulte "[NetApp Active IQ](#)" para obter mais informações.

### Quais são os eventos do sistema de Gestão de Eventos

O sistema de Gerenciamento de Eventos (EMS) coleta dados de eventos de diferentes partes do kernel do ONTAP e fornece mecanismos de encaminhamento de eventos. Esses eventos do ONTAP podem ser relatados como eventos EMS no Unified Manager. O monitoramento e o gerenciamento centralizados facilitam a configuração de eventos críticos do EMS e notificações de alerta com base nesses eventos do EMS.

O endereço do Unified Manager é adicionado como um destino de notificação ao cluster quando você adiciona o cluster ao Unified Manager. Um evento EMS é comunicado assim que o evento ocorre no cluster.

Existem dois métodos para receber eventos EMS no Unified Manager:

- Um certo número de eventos importantes do EMS são relatados automaticamente.
- Você pode se inscrever para receber eventos EMS individuais.

Os eventos EMS gerados pelo Unified Manager são relatados de forma diferente dependendo do método no qual o evento foi gerado:

Funcionalidade	Mensagens EMS automáticas	Mensagens EMS subscritas
Eventos EMS disponíveis	Subconjunto de eventos EMS	Todos os eventos EMS
Nome da mensagem EMS quando acionada	Nome do evento do Unified Manager (convertido do nome do evento EMS)	Não específico no formato "erro EMS recebido". A mensagem detalhada fornece o formato de notação de pontos do evento EMS real
Mensagens recebidas	Assim que o cluster for descoberto	Depois de adicionar cada evento EMS necessário ao Unified Manager e após o próximo ciclo de polling de 15 minutos
Ciclo de vida do evento	O mesmo que outros eventos do Unified Manager: estados novos, reconhecidos, resolvidos e obsoletos	O evento EMS fica obsoleto após o cluster ser atualizado, após 15 minutos, a partir do momento em que o evento foi criado
Captura eventos durante o tempo de inatividade do Unified Manager	Sim, quando o sistema arranca, comunica com cada cluster para adquirir eventos em falta	Não
Detalhes do evento	As ações corretivas sugeridas são importadas diretamente do ONTAP para fornecer resoluções consistentes	Ações corretivas não disponíveis na página Detalhes do evento



Alguns dos novos eventos EMS automáticos são eventos informativos que indicam que um evento anterior foi resolvido. Por exemplo, o evento de informação "Estado do espaço dos constituintes do FlexGroup tudo OK" indica que o evento de erro "componentes do FlexGroup têm problemas de espaço" foi resolvido. Os eventos informativos não podem ser gerenciados usando o mesmo ciclo de vida de eventos que outros tipos de gravidade de eventos, no entanto, o evento fica obsoleto automaticamente se o mesmo volume receber outro evento de erro "problemas de espaço".

### Eventos EMS que são adicionados automaticamente ao Unified Manager

Os seguintes eventos do ONTAP EMS são adicionados automaticamente ao Unified Manager. Esses eventos serão gerados quando acionados em qualquer cluster que o Unified Manager esteja monitorando.

Os eventos EMS a seguir estão disponíveis ao monitorar clusters executando o software ONTAP 9.5 ou superior:

<b>Nome do evento do Unified Manager</b>	<b>Nome do evento EMS</b>	<b>Recurso afetado</b>	<b>Gravidade do Unified Manager</b>
Acesso ao nível da nuvem negado para realocação de agregados	arl.netra.ca.check.failed	Agregado	Erro
Acesso ao nível da nuvem negado para realocação de agregados durante o failover de storage	gb.netra.ca.check.failed	Agregado	Erro
Sincronização de replicação de espelhamento do FabricPool concluída	WAFL.ca.resync.complete	Cluster	Erro
Espaço FabricPool quase cheio	FabricPool.quase.full	Cluster	Erro
Período de carência do NVMe-of iniciado	nvmf.graceperiod.start	Cluster	Aviso
Período de carência NVMe-of Ativo	nvmf.graceperiod.active	Cluster	Aviso
O período de carência do NVMe-of expirou	nvmf.graceperiod.expired	Cluster	Aviso
LUN destruído	lun.destroy	LUN	Informações
Nuvem AWS MetaDataConnFail	Cloud.AWS.metadataConnFail	Nó	Erro
Cloud AWS IAMCredsExpired	Cloud.AWS.iamCredsExpired	Nó	Erro
Nuvem AWS IAMCredsInvalid	Cloud.AWS.iamCredsInvalid	Nó	Erro
Cloud AWS IAMCredsNotFound	Cloud.AWS.iamCredsNotFound	Nó	Erro
Cloud AWS IAMCredsNotInitialized	Cloud.AWS.iamNotInitialized	Nó	Informações

<b>Nome do evento do Unified Manager</b>	<b>Nome do evento EMS</b>	<b>Recurso afetado</b>	<b>Gravidade do Unified Manager</b>
Nuvem AWS IAMRoleInvalid	Cloud.AWS.iamRoleInvalid	Nó	Erro
Nuvem AWS IAMRoleNotFound	Cloud.AWS.iamRoleNotFound	Nó	Erro
Host de nível de nuvem não resolvível	objstore.host.unresolvable	Nó	Erro
Interface de rede de Intercluster de camada de nuvem desativada	objstore.interclusterlifDown	Nó	Erro
Solicitar assinatura incorreta do nível de nuvem	osc.signatureMismatch	Nó	Erro
Uma das NFSv4 piscinas esgotada	Nblade.nfsV4PoolExhaust	Nó	Crítico
Memória do monitor QoS maximizada	qos.monitor.memory.maxed	Nó	Erro
Memória do monitor QoS interrompida	qos.monitor.memory.abated	Nó	Informações
NVMeNS Destroy	NVMeNS.destroy	Namespace	Informações
NVMeNS Online	NVMeNS.offline	Namespace	Informações
NVMeNS Offline	NVMeNS.online	Namespace	Informações
NVMeNS fora do espaço	NVMeNS.out.of.space	Namespace	Aviso
Replicação síncrona fora de sincronização	sms.status.out.of.sync	Relação de SnapMirror	Aviso
Replicação síncrona restaurada	sms.status.in.sync	Relação de SnapMirror	Informações
Falha na ressincronização automática de replicação síncrona	sms.resync.tentativa.falhou	Relação de SnapMirror	Erro



<b>Nome do evento do Unified Manager</b>	<b>Nome do evento EMS</b>	<b>Recurso afetado</b>	<b>Gravidade do Unified Manager</b>
Muitas conexões CIFS	Nblade.cifsManyAuths	SVM	Erro
Conexão CIFS máx. Excedida	Nblade.cifsMaxOpenSam eFile	SVM	Erro
Número máximo de ligação CIFS por utilizador excedido	Nblade.cifsMaxSessPerU srConn	SVM	Erro
Conflito de nomes NetBIOS CIFS	Nblade.cifsNbNameConfl ict	SVM	Erro
Tentativas de conetar compartilhamento CIFS inexistente	Nblade.cifsNoPrivShare	SVM	Crítico
Falha na operação de cópia sombra CIFS	cifs.shadowcopy.failure	SVM	Erro
Vírus encontrado por AV Server	Nblade.vscanVirusDetect ed	SVM	Erro
Nenhuma conexão do servidor AV para verificação de vírus	Nblade.vscanNoScanner Conn	SVM	Crítico
Nenhum servidor AV registado	Nblade.vscanNoRegdSca nner	SVM	Erro
Nenhuma conexão responsiva do servidor AV	Nblade.vscanConnInactiv e	SVM	Informações
Servidor AV demasiado ocupado para aceitar novo pedido de digitalização	Nblade.vscanConnBackPr essure	SVM	Erro
Tentativa de usuário não autorizado para o servidor AV	Nblade.vscanBadUserPriv Access	SVM	Erro
Os constituintes do FlexGroup têm problemas de espaço	FlexGroup.constituintes.h ave.space.issues	Volume	Erro

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do Unified Manager
Estado do espaço dos constituintes do FlexGroup tudo OK	FlexGroup.constituientes.space.status.all.ok	Volume	Informações
Os constituintes do FlexGroup têm problemas inodes	FlexGroup.constituents.have.inodes.issues	Volume	Erro
FlexGroup constituintes inodes Status tudo OK	FlexGroup.constituents.inodes.status.all.ok	Volume	Informações
Volume Logical Space quase cheio	monitor.vol.nearFull.increase	Volume	Aviso
Volume espaço lógico cheio	monitor.vol.full.increase	Volume	Erro
Volume lógico espaço normal	monitor.vol.one.ok.increase	Volume	Informações
Falha na seleção automática do volume do WAFL	WAFL.vol.autoSize.fail	Volume	Erro
WAFL volume AutoSize Done (tamanho automático do volume)	WAFL.vol.autoSize.done	Volume	Informações
Tempo limite de operação do arquivo READDIR do WAFL	WAFL.readdir.expirou	Volume	Erro

### Subscrever eventos ONTAP EMS

Você pode se inscrever para receber eventos do sistema de Gerenciamento de Eventos (EMS) gerados por sistemas instalados com o software ONTAP. Um subconjunto de eventos EMS é relatado automaticamente ao Unified Manager, mas eventos EMS adicionais são relatados somente se você se inscreveu nesses eventos.

#### Antes de começar

Não assine eventos EMS que já foram adicionados ao Unified Manager automaticamente, pois isso pode causar confusão ao receber dois eventos para o mesmo problema.

Você pode se inscrever em qualquer número de eventos EMS. Todos os eventos aos quais você se inscreve são validados e somente os eventos validados são aplicados aos clusters que você está monitorando no Unified Manager. O *Catálogo de Eventos do ONTAP 9 EMS* fornece informações detalhadas para todas as

mensagens do EMS para a versão especificada do software ONTAP 9. Localize a versão apropriada do Catálogo de Eventos *EMS* na página Documentação do produto da ONTAP 9 para obter uma lista dos eventos aplicáveis.

### ["Biblioteca de produtos ONTAP 9"](#)

Você pode configurar alertas para os eventos do ONTAP EMS aos quais você se inscreve e criar scripts personalizados para serem executados para esses eventos.



Se você não receber os eventos do ONTAP EMS aos quais você se inscreveu, pode haver um problema com a configuração DNS do cluster que está impedindo que o cluster chegue ao servidor do Unified Manager. Para resolver esse problema, o administrador do cluster deve corrigir a configuração DNS do cluster e reiniciar o Unified Manager. Isso irá liberar os eventos EMS pendentes para o servidor do Unified Manager.

### Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento > Configuração do evento**.
2. Na página Configuração do evento, clique no botão **Subscrever a eventos EMS**.
3. Na caixa de diálogo assinar eventos EMS, digite o nome do evento EMS do ONTAP ao qual deseja se inscrever.

Para ver os nomes dos eventos EMS aos quais você pode assinar, a partir do shell do cluster ONTAP, você pode usar o `event route show` comando (antes do ONTAP 9) ou o `event catalog show` comando (ONTAP 9 ou posterior).

### ["Como configurar e receber alertas da subscrição de eventos do ONTAP EMS no Active IQ Unified Manager"](#)

4. Clique em **Add**.

O evento EMS é adicionado à lista de eventos EMS subscritos, mas a coluna aplicável ao cluster exibe o status como ""desconhecido"" para o evento EMS que você adicionou.

5. Clique em **Salvar e fechar** para Registrar a assinatura do evento EMS no cluster.
6. Clique em **Inscrever-se para eventos EMS** novamente.

O status ""Sim"" aparece na coluna aplicável ao cluster para o evento EMS que você adicionou.

Se o status não for "Sim", verifique a ortografia do nome do evento ONTAP EMS. Se o nome for inserido incorretamente, você deve remover o evento incorreto e adicionar o evento novamente.

Quando o evento EMS do ONTAP ocorre, o evento é exibido na página Eventos. Pode selecionar o evento para ver detalhes sobre o evento EMS na página de detalhes do evento. Você também pode gerenciar a disposição do evento ou criar alertas para o evento.

## O que acontece quando um evento é recebido

Quando o Unified Manager recebe um evento, ele é exibido na página Dashboard, na página Inventário de Gerenciamento de Eventos, nas guias Summary e Explorer da página Cluster/Performance e na página de inventário específico do objeto (por exemplo,

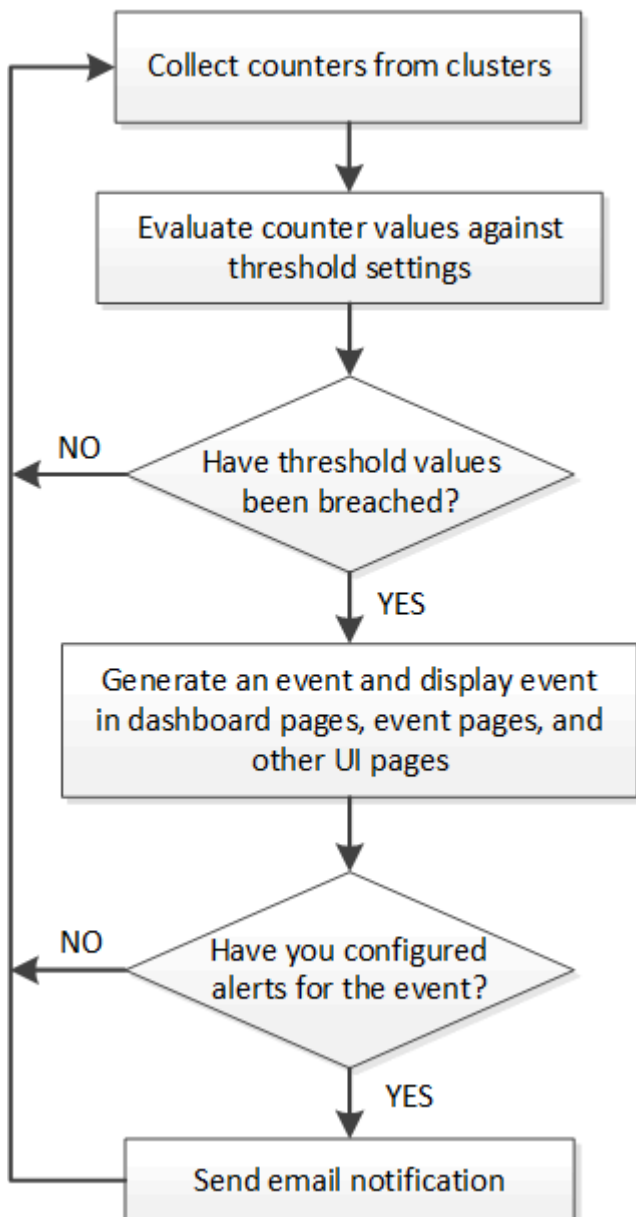
a página volumes/inventário de integridade).

Quando o Unified Manager detecta 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 de alerta, 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.



## Visualização de eventos e detalhes do evento

Você pode exibir detalhes sobre um evento que é acionado pelo Unified Manager para tomar medidas corretivas. Por exemplo, se houver um volume off-line de eventos de integridade, você pode clicar nesse evento para exibir os detalhes e executar ações corretivas.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Os detalhes do evento incluem informações como a origem do evento, a causa do evento e quaisquer notas relacionadas ao evento.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.

Por padrão, a exibição todos os eventos ativos exibe os eventos novos e confirmados (ativos) que foram gerados nos últimos 7 dias que têm um nível de impactos de Incidente ou risco.

2. Se você quiser exibir uma determinada categoria de eventos, por exemplo, eventos de capacidade ou eventos de desempenho, clique em **Exibir** e selecione no menu de tipos de eventos.
3. Clique no nome do evento para o qual deseja exibir os detalhes.

Os detalhes do evento são exibidos na página de detalhes do evento.

## Exibindo eventos não atribuídos

Você pode exibir eventos não atribuídos e, em seguida, atribuir cada um deles a um usuário que pode resolvê-los.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.

Por padrão, eventos novos e confirmados são exibidos na página de inventário do Gerenciamento de Eventos.

2. No painel **filtros**, selecione a opção de filtro **não atribuído** na área **atribuído a**.

## Reconhecer e resolver eventos

Você deve reconhecer um evento antes de começar a trabalhar no problema que gerou o evento para que você não continue a receber notificações de alerta repetidas. Depois de tomar medidas corretivas para um evento específico, você deve marcar o evento como resolvido.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Você pode reconhecer e resolver vários eventos simultaneamente.



Você não pode reconhecer eventos de informações.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.
2. Na lista de eventos, execute as seguintes ações para confirmar os eventos:

Se você quiser...	Faça isso...
Confirme e marque um único evento como resolvido	<ol style="list-style-type: none"><li>a. Clique no nome do evento.</li><li>b. Na página de detalhes do evento, determine a causa do evento.</li><li>c. Clique em <b>confirmar</b>.</li><li>d. Tome as medidas corretivas adequadas.</li><li>e. Clique em <b>Marcar como resolvido</b>.</li></ol>
Confirmar e marcar vários eventos como resolvidos	<ol style="list-style-type: none"><li>a. Determine a causa dos eventos na respectiva página de detalhes do evento.</li><li>b. Selecione os eventos.</li><li>c. Clique em <b>confirmar</b>.</li><li>d. Tome as medidas corretivas apropriadas.</li><li>e. Clique em <b>Marcar como resolvido</b>.</li></ol>

Depois que o evento é marcado como resolvido, o evento é movido para a lista de eventos resolvidos.

3. **Opcional:** Na área **Notas e atualizações**, adicione uma nota sobre como você abordou o evento e clique em **Post**.

## Atribuindo eventos a usuários específicos


Você pode atribuir eventos não atribuídos a você mesmo ou a outros usuários, incluindo usuários remotos. Você pode reatribuir eventos atribuídos a outro usuário, se necessário. Por exemplo, quando ocorrem problemas frequentes em um objeto de storage, você pode atribuir os eventos para esses problemas ao usuário que gerencia esse objeto.

### Antes de começar

- O nome e o ID de e-mail do usuário devem estar configurados corretamente.
- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.
2. Na página de inventário **Gerenciamento de eventos**, selecione um ou mais eventos que você deseja atribuir.
3. Atribua o evento escolhendo uma das seguintes opções:

Se quiser atribuir o evento a...	Então faça isso...
Você mesmo	Clique em <b>Assign to &gt; me</b> .
Outro utilizador	<p>a. Clique em <b>Assign to &gt; Other user</b> (atribuir a).</p> <p>b. Na caixa de diálogo atribuir proprietário, insira o nome de usuário ou selecione um usuário na lista suspensa.</p> <p>c. Clique em <b>Assign</b>.</p> <p>Uma notificação por e-mail é enviada ao usuário.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Se você não inserir um nome de usuário ou selecionar um usuário na lista suspensa e clicar em <b>Assign</b>, o evento permanecerá não atribuído.</p> </div>

## Desativar eventos indesejados

Todos os eventos são ativados por padrão. Você pode desativar eventos globalmente para impedir a geração de notificações para eventos que não são importantes em seu ambiente. Você pode ativar eventos desativados quando quiser retomar o recebimento de notificações para eles.

### Antes de começar

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

Quando você desativa eventos, os eventos gerados anteriormente no sistema são marcados como obsoletos e os alertas configurados para esses eventos não são acionados. Quando você ativa eventos desativados, as notificações para esses eventos são geradas a partir do próximo ciclo de monitoramento.

Quando você desativa um evento para um objeto (por exemplo, o `vol offline` evento) e, depois, ativa o evento, o Unified Manager não gera novos eventos para objetos que ficaram offline quando o evento estava no estado desativado. O Unified Manager gera um novo evento somente quando há uma alteração no estado do objeto após o evento ser reativado.

### Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento > Configuração do evento**.
2. Na página **Configuração do evento**, desative ou ative eventos escolhendo uma das seguintes opções:

Se você quiser...	Então faça isso...
Desativar eventos	<ul style="list-style-type: none"> <li>a. Clique em <b>Desativar</b>.</li> <li>b. Na caixa de diálogo Desativar eventos , selecione a gravidade do evento.</li> <li>c. Na coluna Eventos correspondentes, selecione os eventos que deseja desativar com base na gravidade do evento e clique na seta para a direita para mover esses eventos para a coluna Desativar eventos.</li> <li>d. Clique em <b>Salvar e fechar</b>.</li> <li>e. Verifique se os eventos desativados são apresentados na vista de lista da página Configuração de eventos.</li> </ul>
Ativar eventos	<ul style="list-style-type: none"> <li>a. Marque a caixa de seleção do evento ou eventos que deseja ativar.</li> <li>b. Clique em <b>Ativar</b>.</li> </ul>

## Correção de problemas usando a correção automática do Unified Manager

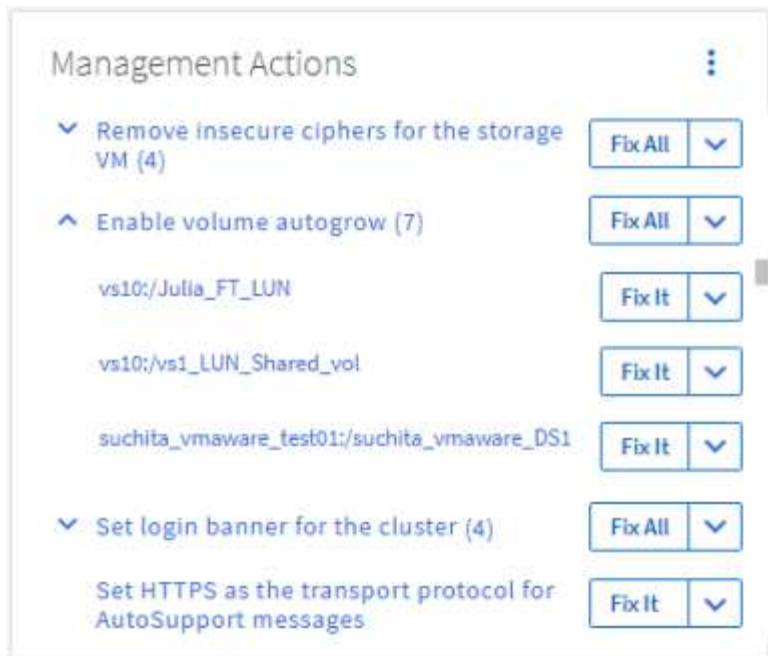
Há certos eventos que o Unified Manager pode diagnosticar minuciosamente e fornecer uma única resolução usando o botão **Fix it**. Quando disponíveis, essas resoluções são exibidas no Painel de instrumentos, na página Detalhes do evento e na seleção análise de carga de trabalho no menu de navegação à esquerda.

A maioria dos eventos tem uma variedade de resoluções possíveis que são exibidas na página de detalhes do evento para que você possa implementar a melhor solução usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP. Uma ação **Fix it** está disponível quando o Unified Manager determinar que há uma única resolução para corrigir o problema e que ele pode ser resolvido usando um comando CLI do ONTAP.

### Passos

1. Para ver eventos que podem ser corrigidos a partir do **Dashboard**, clique em **Dashboard**.





2. Para resolver qualquer um dos problemas que o Unified Manager pode corrigir, clique no botão **Fix it**. Para corrigir um problema que existe em vários objetos, clique no botão **corrigir tudo**.

Para obter informações sobre os problemas que podem ser corrigidos pela correção automática, "[Quais problemas o Unified Manager pode corrigir](#)" consulte .

## Ativar e desativar relatórios de eventos do Active IQ

Os eventos da plataforma Active IQ são gerados e exibidos na interface de usuário do Gerenciador Unificado por padrão. Se você achar que esses eventos são muito "barulhentos" ou que não deseja exibir esses eventos no Unified Manager, poderá desativar esses eventos de serem gerados. Você pode ativá-los posteriormente se quiser continuar recebendo essas notificações.

### Antes de começar

Tem de ter a função Administrador de aplicações.

Quando você desativa esse recurso, o Unified Manager pára de receber eventos da plataforma Active IQ imediatamente.

Quando você ativa esse recurso, o Unified Manager começa a receber eventos da plataforma Active IQ logo após a meia-noite, com base no fuso horário do cluster. A hora de início é baseada em quando o Unified Manager recebe mensagens do AutoSupport de cada cluster.

### Passos

1. No painel de navegação à esquerda, clique em **Geral > Definições da funcionalidade**.
2. Na página **Definições de funcionalidades**, desative ou ative eventos da plataforma Active IQ escolhendo uma das seguintes opções:

Se você quiser...	Então faça isso...
Desativar eventos da plataforma Active IQ	No painel <b>Eventos do Portal Active IQ</b> , mova o botão deslizante para a esquerda.
Ativar eventos da plataforma Active IQ	No painel <b>Eventos do Portal Active IQ</b> , mova o botão deslizante para a direita.

## Carregar um novo ficheiro de regras do Active IQ

O Unified Manager verifica automaticamente um novo arquivo de eventos (regras) do Active IQ e faz o download de um novo arquivo quando há regras mais recentes. No entanto, em sites sem acesso à rede externa, você precisa fazer o upload do arquivo de regras manualmente.



As regras do Active IQ também são chamadas de regras seguras do Config Advisor (CA).

Quando você estiver instalando ou atualizando o Unified Manager para uma versão específica em um site sem conectividade de rede, as regras do Active IQ empacotadas estarão automaticamente disponíveis para upload. No entanto, é recomendável baixar um novo arquivo de regras aproximadamente uma vez por mês no site de suporte da NetApp para garantir que os eventos atualizados sejam gerados e que seus sistemas de storage continuem a ter um desempenho ideal.

### Antes de começar

- O relatório de eventos do portal Active IQ deve estar ativado. Esta funcionalidade está ativada por predefinição. Para obter informações, "[Ativar eventos do portal Active IQ](#)" consulte .
- Você deve baixar o arquivo de regras do site de suporte da NetApp.

O arquivo de regras está localizado em: [https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure\\_rules.zip](https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip)

### Passos

1. Em um computador com acesso à rede, navegue até o site de suporte da NetApp e baixe o arquivo de regras atual .zip.

O pacote de regras inclui o repositório de regras, fontes de dados e um artigo da KB do NetApp.



Em sistemas Windows, em um site sem conectividade de rede, o artigo da KB do NetApp não é empacotado por padrão com o instalador. Você pode baixar o arquivo *secure\_rules.zip* do site de suporte e enviá-lo para visualizar o artigo da KB para todas as regras.

2. Transfira o ficheiro de regras para alguns suportes que pode introduzir na área segura e, em seguida, copie-o para um sistema na área segura.
3. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento > Configuração do evento**.
4. Na página **Configuração do evento**, clique no botão **Upload Rules**.

5. Na caixa de diálogo **Upload Rules**, navegue e selecione o arquivo de regras .zip que você baixou e clique em **Upload**.

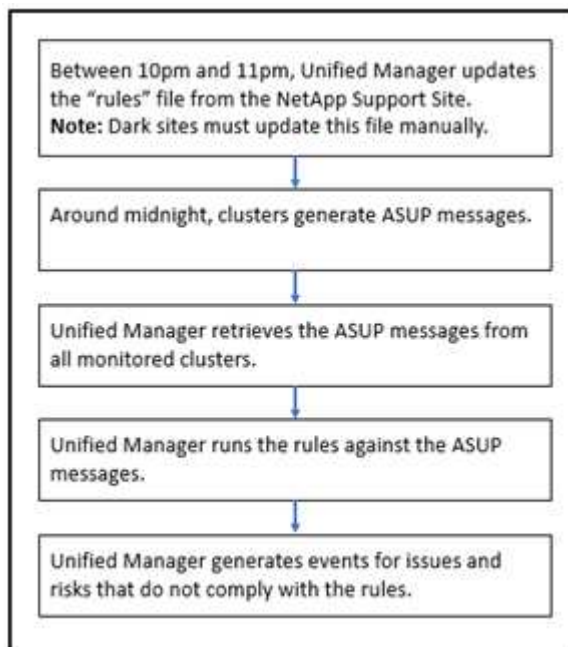
Este processo pode demorar alguns minutos.

O arquivo de regras é descompactado no servidor do Unified Manager. Depois que os clusters gerenciados geram um arquivo AutoSupport após a meia-noite, o Unified Manager verifica os clusters em relação ao arquivo de regras e gera novos eventos de risco e incidente, conforme necessário.

Para obter mais informações, consulte este artigo da base de dados de Conhecimento (KB) "[Como atualizar as regras AIQCA Secure manualmente no Active IQ Unified Manager](#)": .

## Como os eventos da plataforma Active IQ são gerados

Os incidentes e riscos da plataforma Active IQ são convertidos em eventos do Unified Manager, conforme mostrado no diagrama a seguir.

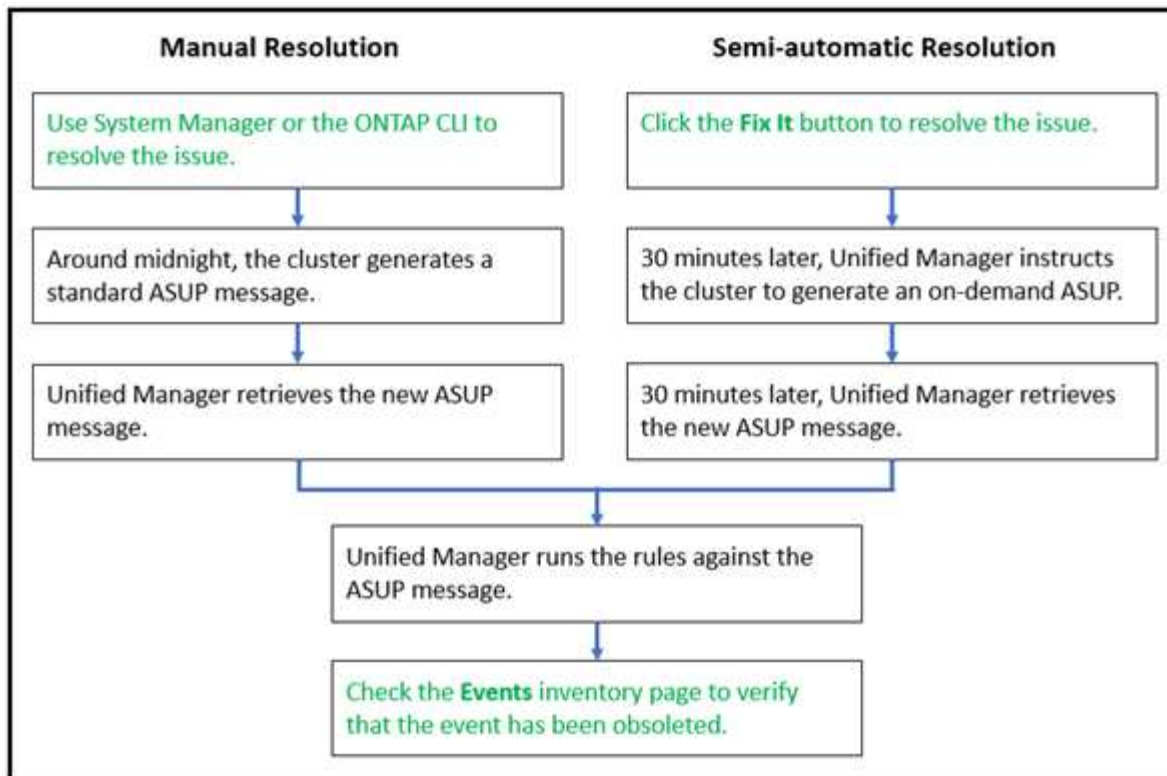


Como você pode ver, o arquivo de regras compilado na plataforma Active IQ é mantido atualizado, as mensagens do cluster AutoSupport são geradas diariamente e o Unified Manager atualiza a lista de eventos diariamente.

## Resolvendo eventos da plataforma Active IQ

Os incidentes e riscos da plataforma Active IQ são semelhantes a outros eventos do Unified Manager porque eles podem ser atribuídos a outros usuários para resolução e têm os mesmos estados disponíveis. No entanto, quando você resolve esses tipos de eventos usando o botão **Fix it**, você pode verificar a resolução em horas.

O diagrama a seguir mostra as ações que você deve executar (em verde) e a ação que o Gerenciador Unificado executa (em preto) ao resolver eventos que foram gerados a partir da plataforma Active IQ.



Ao executar uma resolução manual, você deve fazer login no Gerenciador do sistema ou na interface da linha de comando do ONTAP para corrigir o problema. Você poderá verificar o problema somente depois que o cluster gerar uma nova mensagem do AutoSupport à meia-noite.

Ao executar uma resolução semi-automática usando o botão **Fix it**, você pode verificar se a correção foi bem-sucedida em poucas horas.

## Configuração das configurações de retenção de eventos

Você pode especificar o número de meses em que um evento é retido no servidor do Unified Manager antes de ser excluído automaticamente.

### Antes de começar

Tem de ter a função Administrador de aplicações.

A retenção de eventos por mais de 6 meses pode afetar o desempenho do servidor e não é recomendada.

### Passos

1. No painel de navegação esquerdo, clique em **Geral > retenção de dados**.
2. Na página **retenção de dados**, selecione o controle deslizante na área retenção de eventos e mova-o para o número de meses em que os eventos devem ser mantidos e clique em **Salvar**.

## O que é uma janela de manutenção do Unified Manager

Você define uma janela de manutenção do Unified Manager para suprimir eventos e alertas para um período de tempo específico quando você agendar a manutenção do cluster e não deseja receber uma série de notificações indesejadas.

Quando a janela de manutenção é iniciada, um evento "janela de manutenção de objetos iniciada" é publicado na página de inventário do Gerenciamento de Eventos. Este evento fica obsoleto automaticamente quando a janela de manutenção termina.

Durante uma janela de manutenção, os eventos relacionados a todos os objetos nesse cluster ainda são gerados, mas eles não aparecem em nenhuma das páginas da IU, e nenhum alerta ou outro tipo de notificação são enviados para esses eventos. No entanto, você pode exibir os eventos que foram gerados para todos os objetos de armazenamento durante uma janela de manutenção selecionando uma das opções Exibir na página de inventário Gerenciamento de Eventos.

Você pode agendar uma janela de manutenção para ser iniciada no futuro, alterar as horas de início e término de uma janela de manutenção agendada e cancelar uma janela de manutenção agendada.

### **Agendar uma janela de manutenção para desativar as notificações de eventos do cluster**

Se você tiver um tempo de inatividade planejado para um cluster, por exemplo, para atualizar o cluster ou mover um dos nós, poderá suprimir os eventos e alertas que normalmente seriam gerados durante esse período agendando uma janela de manutenção do Unified Manager.

#### **Antes de começar**

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

Durante uma janela de manutenção, os eventos relacionados a todos os objetos nesse cluster ainda são gerados, mas eles não aparecem na página de eventos e nenhum alerta ou outro tipo de notificação são enviados para esses eventos.

A hora que você inserir para a janela de manutenção é baseada na hora no servidor do Unified Manager.

#### **Passos**

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração do cluster**.
2. Na coluna **Maintenance Mode** do cluster, selecione o botão deslizante e mova-o para a direita.

É apresentada a janela de calendário.

3. Selecione a data e a hora de início e fim da janela de manutenção e clique em **Apply**.

A mensagem "agendado" aparece ao lado do botão deslizante.

Quando a hora de início é atingida, o cluster entra no modo de manutenção e é gerado um evento "janela de manutenção de objetos iniciada".

### **Alterar ou cancelar uma janela de manutenção agendada**

Se você tiver configurado uma janela de manutenção do Unified Manager para ocorrer no futuro, poderá alterar as horas de início e término ou cancelar a ocorrência da janela de manutenção.

#### **Antes de começar**

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

O cancelamento de uma janela de manutenção atualmente em execução é útil se você tiver concluído a manutenção do cluster antes da hora de término da janela de manutenção programada e quiser começar a receber eventos e alertas do cluster novamente.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração do cluster**.
2. Na coluna **Maintenance Mode** para o cluster:

Se você quiser...	Execute esta etapa...
Altere o período de tempo para uma janela de manutenção agendada	<ol style="list-style-type: none"><li>a. Clique no texto "agendado" ao lado do botão deslizante.</li><li>b. Altere a data e hora de início e/ou fim e clique em <b>aplicar</b>.</li></ol>
Estenda o comprimento de uma janela de manutenção ativa	<ol style="list-style-type: none"><li>a. Clique no texto "Ativo" ao lado do botão deslizante.</li><li>b. Altere a data e a hora de término e clique em <b>Apply</b>.</li></ol>
Cancelar uma janela de manutenção agendada	Selecione o botão deslizante e mova-o para a esquerda.
Cancelar uma janela de manutenção ativa	Selecione o botão deslizante e mova-o para a esquerda.

### Visualização de eventos que ocorreram durante uma janela de manutenção

Se necessário, você pode exibir os eventos que foram gerados para todos os objetos de armazenamento durante uma janela de manutenção do Unified Manager. A maioria dos eventos aparecerá no estado Obsoleto assim que a janela de manutenção estiver concluída e todos os recursos do sistema estiverem em backup e em execução.

#### Antes de começar

Pelo menos uma janela de manutenção deve ter sido concluída antes de quaisquer eventos estarem disponíveis.

Os eventos que ocorreram durante uma janela de manutenção não aparecem na página de inventário do Gerenciamento de Eventos por padrão.

### Passos

1. No painel de navegação esquerdo, clique em **Eventos**.

Por padrão, todos os eventos ativos (novos e confirmados) são exibidos na página de inventário do Gerenciamento de Eventos.

2. No painel Exibir, selecione a opção **todos os eventos gerados durante a manutenção**.

A lista de eventos trigados durante os últimos 7 dias de todas as sessões de janela de manutenção e de todos os clusters é exibida.

3. Se houver várias janelas de manutenção para um único cluster, você pode clicar no ícone de calendário **hora ativada** e selecionar o período de tempo para os eventos da janela de manutenção que você está interessado em visualizar.

## Gerenciamento de eventos de recursos do sistema host

O Unified Manager inclui um serviço que monitora problemas de recursos no sistema de host no qual o Unified Manager está instalado. Problemas como falta de espaço disponível em disco ou falta de memória no sistema host podem acionar eventos da estação de gerenciamento que são exibidos como mensagens de banner na parte superior da interface do usuário.

Os eventos da estação de gerenciamento indicam um problema com o sistema host no qual o Unified Manager está instalado. Exemplos de problemas de estação de gerenciamento incluem espaço em disco com pouca execução no sistema host; falta do Unified Manager um ciclo regular de coleta de dados; e não conclusão ou conclusão tardia da análise estatística porque a próxima pesquisa de coleta foi iniciada.

Ao contrário de todas as outras mensagens de evento do Unified Manager, esses avisos específicos da estação de gerenciamento e eventos críticos são exibidos em mensagens de banner.

### Passo

1. Para visualizar as informações de eventos da estação de gerenciamento, execute estas ações:

Se você quiser...	Faça isso...
Ver detalhes do evento	Clique no banner de evento para exibir a página de detalhes do evento que inclui soluções sugeridas para o problema.
Veja todos os eventos da estação de gerenciamento	<ol style="list-style-type: none"><li>a. No painel de navegação esquerdo, clique em <b>Gerenciamento de eventos</b>.</li><li>b. No painel filtros na página Inventário de Gerenciamento de Eventos, clique na caixa de Gerenciamento da Estação na lista tipo de origem.</li></ol>

## Compreender mais sobre eventos

Compreender os conceitos sobre eventos ajuda você a gerenciar seus clusters e objetos de cluster com eficiência e a definir alertas adequadamente.

### Definições de estado do evento

O estado de um evento ajuda a identificar se é necessária uma ação corretiva adequada. Um evento pode ser novo, reconhecido, resolvido ou Obsoleto. Observe que eventos novos e reconhecidos são considerados eventos ativos.

Os estados do evento são os seguintes:

- **Novo**

O estado de um novo evento.

- **Reconhecido**

O estado de um evento quando você o reconheceu.

- **Resolvido**

O estado de um evento quando ele é marcado como resolvido.

- **Obsoleto**

O estado de um evento quando ele é corrigido automaticamente ou quando a causa do evento não é mais válida.



Não é possível reconhecer ou resolver um evento obsoleto.

#### **Exemplo de estados diferentes de um evento**

Os exemplos a seguir ilustram as alterações manuais e automáticas do estado do evento.

Quando o Cluster de Eventos não alcançável é acionado, o estado de evento é novo. Quando você reconhece o evento, o estado do evento muda para confirmado. Quando você tiver tomado uma ação corretiva apropriada, você deve marcar o evento como resolvido. O estado do evento muda então para resolvido.

Se o evento Cluster Not reachable for gerado devido a uma falha de energia, então, quando a energia for restaurada, o cluster começa a funcionar sem qualquer intervenção do administrador. Portanto, o evento Cluster Not reachable não é mais válido e o estado do evento muda para Obsoleto no próximo ciclo de monitoramento.

O Unified Manager envia um alerta quando um evento está no estado Obsoleto ou resolvido. A linha de assunto do e-mail e o conteúdo de um alerta fornecem informações sobre o estado do evento. Uma armadilha SNMP também inclui informações sobre o estado do evento.

#### **Descrição dos tipos de gravidade do evento**

Cada evento é associado a um tipo de gravidade para ajudá-lo a priorizar os eventos que exigem ação corretiva imediata.

- **Crítica**

Ocorreu um problema que pode levar à interrupção do serviço se não forem tomadas medidas corretivas imediatamente.

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

- **Erro**

A origem do evento ainda está em execução; no entanto, é necessária uma ação corretiva para evitar interrupção do serviço.



- **Aviso**

A origem do evento experimentou uma ocorrência que você deve estar ciente ou um contador de desempenho de 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 de desempenho 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 detecta uma alteração de configuração.

## **Descrição dos níveis de impactos do evento**

Cada evento é associado a um nível de impactos (Incidente, risco, evento ou Atualização) para ajudá-lo a priorizar os eventos que exigem ação corretiva imediata.

- **Incidente**

Um incidente é um conjunto de eventos que podem fazer com que um cluster pare de fornecer dados ao cliente e fique sem espaço para armazenar dados. Os eventos com um nível de impactos de Incidente são os mais graves. Devem ser tomadas medidas corretivas imediatas para evitar interrupções no serviço.

- **Risco**

Um risco é um conjunto de eventos que podem potencialmente fazer com que um cluster pare de fornecer dados ao cliente e fique sem espaço para armazenar dados. Eventos com um nível de impacto de risco podem causar interrupções no serviço. Pode ser necessária uma ação corretiva.

- **Evento**

Um evento é uma alteração de estado ou status de objetos de armazenamento e seus atributos. Os eventos com um nível de impactos de evento são informativos e não requerem ação corretiva.

- **Upgrade**

Os eventos de atualização são um tipo específico de evento relatado na plataforma Active IQ. Esses eventos identificam problemas em que a resolução exige que você atualize o software ONTAP, o firmware do nó ou o software do sistema operacional (para avisos de segurança). Você pode querer executar ações corretivas imediatas para alguns desses problemas, enquanto outros problemas podem esperar até a próxima manutenção programada.

## **Descrição das áreas de impactos de eventos**

Os eventos são categorizados em seis áreas de impactos (disponibilidade, capacidade, configuração, desempenho, proteção e segurança) para que você possa se concentrar

nos tipos de eventos pelos quais você é responsável.

- **Disponibilidade**

Os eventos de disponibilidade notificam se um objeto de armazenamento ficar offline, se um serviço de protocolo ficar inativo, se ocorrer um problema com failover de armazenamento ou se ocorrer um problema com hardware.

- **Capacidade**

Os eventos de capacidade notificam você se agregados, volumes, LUNs ou namespaces estão próximos ou atingiram um limite de tamanho, ou se a taxa de crescimento é incomum para o seu ambiente.

- **Configuração**

Os eventos de configuração informam sobre a descoberta, exclusão, adição, remoção ou renomeação de seus objetos de armazenamento. Os eventos de configuração têm um nível de impactos de evento e um tipo de informação de gravidade.

- **Desempenho**

Os eventos de desempenho notificam você sobre as condições de recursos, configuração ou atividade no cluster que podem afetar negativamente a velocidade de entrada ou recuperação de armazenamento de dados em seus objetos de armazenamento monitorados.

- **Proteção**

Eventos de proteção notificam você sobre incidentes ou riscos envolvendo relacionamentos do SnapMirror, problemas com a capacidade de destino, problemas com relacionamentos do SnapVault ou problemas com tarefas de proteção. Todos os objetos ONTAP (especialmente agregados, volumes e SVMs) que hospedam volumes secundários e relacionamentos de proteção são categorizados na área de impacto de proteção.

- **Segurança**

Os eventos de segurança notificam a segurança dos clusters do ONTAP, das máquinas virtuais de armazenamento (SVMs) e dos volumes com base nos parâmetros definidos no "[Guia de endurecimento de segurança da NetApp para ONTAP 9](#)".

Além disso, essa área inclui eventos de atualização que são relatados da plataforma Active IQ.

### **Como o status do objeto é calculado**

O status do objeto é determinado pelo evento mais grave que atualmente detém um estado novo ou reconhecido. Por exemplo, se um status de objeto for erro, um dos eventos do objeto tem um tipo de gravidade de erro. Quando a ação corretiva tiver sido tomada, o estado do evento passa para resolvido.

### **Detalhes do gráfico de eventos de desempenho dinâmico**

Para eventos de desempenho dinâmico, a seção Diagnóstico do sistema da página de detalhes do evento lista as principais cargas de trabalho com a maior latência ou uso do componente do cluster que está em disputa.

As estatísticas de desempenho baseiam-se no tempo em que o evento de desempenho foi detetado até a última vez que o evento foi analisado. Os gráficos também exibem estatísticas históricas de desempenho para o componente do cluster que está em disputa.

Por exemplo, você pode identificar workloads com alta utilização de um componente para determinar qual workload mover para um componente menos utilizado. Mover a carga de trabalho reduziria a quantidade de trabalho no componente atual, possivelmente deixando o componente fora da contenção. Na parte superior desta secção encontra-se a hora e o intervalo de datas em que um evento foi detetado e analisado pela última vez. Para eventos ativos (novos ou reconhecidos), a última hora analisada é atualizada.

Os gráficos de latência e atividade exibem os nomes das principais cargas de trabalho quando você passa o cursor sobre o gráfico. Clicar no menu tipo de carga de trabalho à direita do gráfico permite classificar as cargas de trabalho com base em sua função no evento, incluindo *sharks*, *bullies* ou *vitimas*, e exhibe detalhes sobre sua latência e seu uso no componente de cluster em disputa. Você pode comparar o valor real com o valor esperado para ver quando o workload estava fora do intervalo esperado de latência ou uso. Para obter informações, "[Tipos de workloads monitorados pelo Unified Manager](#)" consulte .



Quando você classifica por desvio de pico na latência, as cargas de trabalho definidas pelo sistema não são exibidas na tabela, porque a latência se aplica somente a cargas de trabalho definidas pelo usuário. As cargas de trabalho com valores de latência muito baixos não são exibidas na tabela.

Para obter mais informações sobre os limites de desempenho dinâmico, "[Analisando eventos a partir de limites dinâmicos de desempenho](#)" consulte .

Para obter informações sobre como o Unified Manager classifica as cargas de trabalho e determina a ordem de classificação, "[Como o Unified Manager determina o impacto no desempenho de um evento](#)" consulte .

Os dados nos gráficos mostram 24 horas de estatísticas de desempenho antes da última vez em que o evento foi analisado. Os valores reais e os valores esperados para cada workload baseiam-se no tempo em que a carga de trabalho foi envolvida no evento. Por exemplo, uma carga de trabalho pode se envolver em um evento depois que o evento foi detetado, portanto, suas estatísticas de desempenho podem não corresponder aos valores no momento da deteção de eventos. Por padrão, as cargas de trabalho são classificadas por desvio de pico (mais alto) na latência.



Como o Unified Manager retém no máximo 30 dias de dados de eventos e performance históricos de 5 minutos, se o evento tiver mais de 30 dias, nenhum dado de performance será exibido.

## • Coluna de ordenação de carga de trabalho

### ◦ Gráfico de latência

Exibe o impactos do evento na latência da carga de trabalho durante a última análise.

### ◦ Coluna de uso de componentes

Exibe detalhes sobre o uso do workload do componente do cluster na contenção. Nos gráficos, o uso real é uma linha azul. Uma barra vermelha destaca a duração do evento, desde o tempo de deteção até o último tempo analisado. Para obter mais informações, "[Valores de medição de performance de workload](#)" consulte .



Para o componente de rede, uma vez que as estatísticas de desempenho da rede provêm de atividades fora do cluster, esta coluna não é apresentada.

- **Uso do componente**

Exibe o histórico de utilização, em porcentagem, para os componentes de processamento de rede, Data Processing e agregado ou o histórico de atividade, em porcentagem, para o componente do grupo de políticas de QoS. O gráfico não é exibido para os componentes de rede ou interconexão. Você pode apontar para as estatísticas para visualizar as estatísticas de uso em um ponto específico no tempo.

- \* Total escrever MB/s História\*

Somente para o componente recursos do MetroCluster, a mostra a taxa de transferência de gravação total, em megabytes por segundo (Mbps), para todas as cargas de trabalho de volume que estão sendo espelhadas para o cluster de parceiros em uma configuração do MetroCluster.

- **Histórico do evento**

Exibe linhas sombreadas em vermelho para indicar os eventos históricos para o componente em disputa. Para eventos obsoletos, o gráfico exibe eventos que ocorreram antes do evento selecionado ser detetado e depois de resolvido.

## **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 análise de carga de trabalho para ver se o evento de mudança 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 (MB/s 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 detectar 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 detectará o evento.

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

São apresentadas a versão anterior e a nova versão.

## Lista de eventos e tipos de gravidade

Você pode usar a lista de eventos para se familiarizar mais com categorias de eventos, nomes de eventos e o tipo de gravidade de cada evento que você pode ver no Unified Manager. Os eventos são listados em ordem alfabética por categoria de objeto.

### Agregar eventos

Os eventos agregados fornecem informações sobre o status dos agregados para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Um asterisco (\*) identifica eventos EMS que foram convertidos para eventos do Unified Manager.

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Agregar Offline (ocumEvtAggregateState Offline)	Incidente	Agregado	Crítico
Falha agregada (ocumEvtAggregateState Failed)	Incidente	Agregado	Crítico
Agregado restrito (ocumEvtAggregateStates Restricted)	Risco	Agregado	Aviso
Reconstrução de agregados (ocumEvtAggregateRaidS tatesReconstructing)	Risco	Agregado	Aviso
Agregado degradado (ocumEvtAggregateRaidS tatement Degraded)	Risco	Agregado	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Camada de nuvem parcialmente acessível (ocumEventCloudTierPartiallyReachable)	Risco	Agregado	Aviso
Camada de nuvem inacessível (ocumEventCloudTierUnreachable)	Risco	Agregado	Erro
Acesso ao nível de nuvem negado para realocação agregada *(arINetraCaCheckFailed)	Risco	Agregado	Erro
Acesso ao nível de nuvem negado para realocação de agregados durante failover de armazenamento *(gbNetraCaCheckFailed)	Risco	Agregado	Erro
MetroCluster agregado deixado para trás (ocumEvtMetroClusterAggregateLeftBehind)	Risco	Agregado	Erro
Espelhamento de agregados MetroCluster degradado(ocumEvtMetroClusterAggregateMirrorDegraded)	Risco	Agregado	Erro

#### Área de impactos: Capacidade

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Agregado espaço quase cheio (ocumEvtAggregateNearlyFull)	Risco	Agregado	Aviso
Agregado espaço cheio (ocumEvtAggregateFull)	Risco	Agregado	Erro

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Agregar dias até completo (ocumEvtAggregateDaysUntilFullSoon)	Risco	Agregado	Erro
Agregado overcommitted (ocumEvtAggregateOvercommitted)	Risco	Agregado	Erro
Agregado quase sobrecomprometido (ocumEvtAggregateAlmostOvercommitted)	Risco	Agregado	Aviso
Reserva de Snapshot agregada completa (ocumEvtAggregateSnapshotReserveFull)	Risco	Agregado	Aviso
Taxa de crescimento agregado anormal (ocumEvtAggregateGrowthRateAbnormal)	Risco	Agregado	Aviso

#### Área de impactos: Configuração

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Agregado descoberto (não aplicável)	Evento	Agregado	Informações
Agregado renomeado (não aplicável)	Evento	Agregado	Informações
Agregado excluído (não aplicável)	Evento	Nó	Informações

#### Área de impactos: Desempenho

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite crítico de IOPS agregado violado (ocumAggregateIopsIncident)	Incidente	Agregado	Crítico

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite de aviso de IOPS agregado violado (ocumAggregateIopsWarning)	Risco	Agregado	Aviso
Agregado MB/s limite crítico violado(ocumAggregateMbpsIncidente)	Incidente	Agregado	Crítico
Agregado MB/s limiar de aviso violado(ocumAggregateMbpsWarning)	Risco	Agregado	Aviso
Limite crítico de latência agregado violado (ocumAggregateLatencyIncident)	Incidente	Agregado	Crítico
Limite de aviso de latência agregada violado (ocumAggregateLatencyWarning)	Risco	Agregado	Aviso
Capacidade de desempenho agregado usada limiar crítico violado (ocumAggregatePerfCapacityUsedIncident)	Incidente	Agregado	Crítico
Limite de aviso de capacidade de desempenho agregado usado violado (ocumAggregatePerfCapacityUsedWarning)	Risco	Agregado	Aviso
Limite crítico de utilização de agregados violado (ocumAggregateUtilizationIncident)	Incidente	Agregado	Crítico



Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Limite de aviso de utilização de agregados violado (ocumAggregateUtilizationWarning)	Risco	Agregado	Aviso
Limite excedido de utilização excessiva de discos agregados (ocumAggregateDisksOverUtilizedWarning)	Risco	Agregado	Aviso
Limite dinâmico agregado violado (ocumAggregateDynamicEventWarning)	Risco	Agregado	Aviso

### Eventos de cluster

Os eventos do cluster fornecem informações sobre o status dos clusters, o que permite monitorar os clusters em busca de possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento, o nome da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Um asterisco (\*) identifica eventos EMS que foram convertidos para eventos do Unified Manager.

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Cluster não possui discos de reserva (ocumEvtDisksNoSpares)	Risco	Cluster	Aviso
Cluster não alcançável (ocumEvtClusterUnreachable)	Risco	Cluster	Erro
Falha no monitoramento de cluster (ocumEvtClusterMonitoringFailed)	Risco	Cluster	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limites de capacidade de licença de cluster FabricPool violados (ocumEvtExternalCapacityTierSpaceFull)	Risco	Cluster	Aviso
Período de carência NVMe-of iniciado *(nvmfGracePeriodStart)	Risco	Cluster	Aviso
Período de carência NVMe-of Ativo *(nvmfGracePeriodActive)	Risco	Cluster	Aviso
Período de carência de NVMe-of expirado *(nvmfGracePeriodExpired)	Risco	Cluster	Aviso
Janela Manutenção Objeto iniciada(objectMaintenance WindowStarted)	Evento	Cluster	Crítico
Janela Manutenção Objeto terminado(objectMaintenance WindowEnded)	Evento	Cluster	Informações
Discos de reposição MetroCluster deixados para trás (ocumEvtSpareDiskLeftBehind)	Risco	Cluster	Erro
Comutação automática não planejada do MetroCluster desativada(ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Risco	Cluster	Aviso
Senha do usuário do cluster alterada *(cluster.passwd.changed)	Evento	Cluster	Informações

**Área de impactos: Capacidade**

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite de desequilíbrio da capacidade do cluster violado (ocumConformanteNodeImbalanceWarning)	Risco	Cluster	Aviso
Planejamento de camada de nuvem de cluster (clusterCloudTierPlanningWarning)	Risco	Cluster	Aviso
Replicação de espelho FabricPool Resync concluída (wafCaResyncComplete)	Evento	Cluster	Aviso
FabricPool espaço quase cheio * (fabricpoolNearlyFull)	Risco	Cluster	Erro

**Área de impactos: Configuração**

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Nó adicionado (não aplicável)	Evento	Cluster	Informações
Nó removido (não aplicável)	Evento	Cluster	Informações
Cluster removido (não aplicável)	Evento	Cluster	Informações
Falha na adição de cluster (não aplicável)	Evento	Cluster	Erro
Nome do cluster alterado (não aplicável)	Evento	Cluster	Informações
EMS de emergência recebido (não aplicável)	Evento	Cluster	Crítico

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
EMS crítico recebido (não aplicável)	Evento	Cluster	Crítico
Alerta EMS recebido (não aplicável)	Evento	Cluster	Erro
Erro EMS recebido (não aplicável)	Evento	Cluster	Aviso
Aviso EMS recebido (não aplicável)	Evento	Cluster	Aviso
Depurar EMS recebido (não aplicável)	Evento	Cluster	Aviso
Aviso EMS recebido (não aplicável)	Evento	Cluster	Aviso
EMS informativo recebido (não aplicável)	Evento	Cluster	Aviso

Os eventos do ONTAP EMS são categorizados em três níveis de gravidade de evento do Unified Manager.

Nível de gravidade do evento do Unified Manager	Nível de gravidade do evento EMS do ONTAP
Crítico	Emergência Crítico
Erro	Alerta
Aviso	Erro Aviso Depurar Aviso Informativo

**Área de impactos: Desempenho**

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite de desequilíbrio de carga do cluster violado()	Risco	Cluster	Aviso
Limite crítico de IOPS do cluster violado (ocumClusterIopsIncident)	Incidente	Cluster	Crítico
Limite de aviso de IOPS do cluster violado (ocumClusterIopsWarning)	Risco	Cluster	Aviso
Limite crítico de MB/s de cluster violado(ocumClusterMbpsIncident)	Incidente	Cluster	Crítico
Limite de aviso do cluster MB/s violado(ocumClusterMbpsWarning)	Risco	Cluster	Aviso
Limite dinâmico do cluster violado (ocumClusterDynamicEventWarning)	Risco	Cluster	Aviso

**Área de impactos: Segurança**

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
AutoSupport HTTPS Transport Disabled(ocumClusterASUPHttpsConfiguredDisabled)	Risco	Cluster	Aviso
Encaminhamento de logs não criptografado (ocumClusterAuditLogUnEncrypted)	Risco	Cluster	Aviso
Usuário Admin local padrão habilitado(ocumClusterDefaultAdminEnabled)	Risco	Cluster	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Modo FIPS desativado (ocumClusterFipsDisabled)	Risco	Cluster	Aviso
Login Banner Disabled(ocumClusterLoginBannerDisabled)	Risco	Cluster	Aviso
Login Banner alterado(ocumClusterLoginBannerChanged)	Risco	Cluster	Aviso
Destinos de encaminhamento de logs alterados(ocumLogForwardDestinationsChanged)	Risco	Cluster	Aviso
Nomes de servidor NTP alterados(ocumNtpServerNamesChanged)	Risco	Cluster	Aviso
Contagem de servidor NTP é baixa (securityConfigNTPServerCountLowRisk)	Risco	Cluster	Aviso
Comunicação por pares de cluster não criptografada (ocumClusterPeerEncryptionDisabled)	Risco	Cluster	Aviso
SSH está usando Ciphers inseguros(ocumClusterSSHInsecure)	Risco	Cluster	Aviso
Protocolo Telnet ativado (ocumClusterTelnetEnabled)	Risco	Cluster	Aviso
Senhas de algumas contas de usuário do ONTAP usam a função hash MD5 menos segura(ocumClusterMD5PasswordHashUsed)	Risco	Cluster	Aviso

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Cluster usa certificado auto-assinado (ocumClusterSelfSignedCertificate)	Risco	Cluster	Aviso
O Shell remoto de cluster está ativado (ocumClusterRshDisabled)	Risco	Cluster	Aviso
Certificado de cluster prestes a expirar (ocumEvtClusterCertificateAboutToExpire)	Risco	Cluster	Aviso
Certificado de cluster expirado (ocumEvtClusterCertificateExpired)	Risco	Cluster	Erro

### Eventos de discos

Os eventos do Disks fornecem informações sobre o status dos discos para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Discos flash - blocos de reposição quase consumidos(ocumEvtClusterFlashDiskFewerSporeBlockError)	Risco	Cluster	Erro
Discos flash - sem blocos de reposição(ocumEvtClusterFlashDiskNoSporeBlockCritical)	Incidente	Cluster	Crítico

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Alguns discos não atribuídos (ocumEvtClusterUnassignedDisksNome)	Risco	Cluster	Aviso
Alguns discos falhados (ocumEvtDisksSomeFailed)	Incidente	Cluster	Crítico

### Eventos de cercos

Os eventos de compartimentos fornecem informações sobre o status dos compartimentos de gaveta de disco em seu data center para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Ventiladores de prateleira de disco falharam (ocumEvtShelfFanFailed)	Incidente	Compartimento de armazenamento	Crítico
Falha nas fontes de alimentação da prateleira de disco (ocumEvtShelfPowerSupplyFailed)	Incidente	Compartimento de armazenamento	Crítico
Multipath não configurado (ocumDiskShelfConnectivityNotInMultiPath)  Este evento não se aplica a:  <ul style="list-style-type: none"> <li>• Clusters que estão em uma configuração MetroCluster</li> <li>• As seguintes plataformas: FAS2554, FAS2552, FAS2520 e FAS2240</li> </ul>	Risco	Nó	Aviso



Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Falha do caminho da prateleira de disco (ocumDiskShelfConnectivityPathFailure)	Risco	Compartimento de armazenamento	Aviso

#### Área de impactos: Configuração

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Compartimento de disco descoberto (não aplicável)	Evento	Nó	Informações
Compartimentos de disco removidos (não aplicável)	Evento	Nó	Informações

#### Eventos de fãs

Os eventos de fãs fornecem informações sobre os fãs de status nos nós do seu data center para que você possa monitorar se há problemas em potencial. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Um ou mais fãs falidos(ocumEvtFansOneOrMoreFailed)	Incidente	Nó	Crítico

#### Eventos do cartão flash

Os eventos do cartão flash fornecem informações sobre o status das placas flash instaladas nos nós do data center para que você possa monitorar se há problemas em potencial. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Flash Cards Offline (ocumEvtFlashCardOffline)	Incidente	Nó	Crítico

### Inodes eventos

Os eventos do inode fornecem informações quando o inode está cheio ou quase cheio para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Capacidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Inodes quase Full (ocumEvtInodesAlmostFull)	Risco	Volume	Aviso
Inodes Full (ocumEvtInodesFull)	Risco	Volume	Erro

### Eventos de interface de rede (LIF)

Os eventos de interface de rede fornecem informações sobre o status de sua interface de rede (LIFs), para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Status da interface de rede para baixo (ocumEvtLifStatusDown)	Risco	Interface	Erro
Status da interface de rede FC/FCoE para baixo (ocumEvtFCLifStatusDown)	Risco	Interface	Erro

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Failover de interface de rede não possível (ocumEvtLifFailoverNotPossible)	Risco	Interface	Aviso
Interface de rede não na porta de casa (ocumEvtLifNotAtHomePort)	Risco	Interface	Aviso

#### Área de impactos: Configuração

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Rota da interface de rede não configurada (não aplicável)	Evento	Interface	Informações

#### Área de impactos: Desempenho

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Limite crítico de MB/s violado(ocumNetworkLifMbpsIncident)	Incidente	Interface	Crítico
Limite de aviso de MB/s de interface de rede violado(ocumNetworkLifMbpsWarning)	Risco	Interface	Aviso
Limite crítico de MB/s de interface de rede FC violado(ocumFcpLifMbpsIncident)	Incidente	Interface	Crítico
Limite de aviso de MB/s de interface de rede FC violado(ocumFcpLifMbpsWarning)	Risco	Interface	Aviso
Interface de rede NVMe FC limiar crítico violado (ocumNvmfFcLifMbpsIncident)	Incidente	Interface	Crítico

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Limite de aviso de MB/s da interface de rede NVMe FC violado(ocumNvmfFcLifMbpsWarning)	Risco	Interface	Aviso

## Eventos LUN

Os eventos LUN fornecem informações sobre o status dos LUNs, para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

### Área de impactos: Disponibilidade

Um asterisco (\*) identifica eventos EMS que foram convertidos para eventos do Unified Manager.

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
LUN Offline(ocumEvtLunOffline)	Incidente	LUN	Crítico
LUN destruído *(lunDestroy)	Evento	LUN	Informações
LUN mapeado com sistema operacional não suportado no igroup(igroupUnsupportedOsType)	Incidente	LUN	Aviso
Caminho Ativo único para acessar LUN(ocumEvtLunSingleActivePath)	Risco	LUN	Aviso
Sem caminhos ativos para acessar LUN(ocumEvtLunNotReachable)	Incidente	LUN	Crítico
Sem caminhos otimizados para acessar LUN(ocumEvtLunOptimizedPathInactive)	Risco	LUN	Aviso

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Sem caminhos para acessar LUN do HA Partner(ocumEvtLunHaPathInactive)	Risco	LUN	Aviso
Nenhum caminho para acessar LUN de um nó no par HA (ocumEvtLunNodePathStatusDown)	Risco	LUN	Erro

#### Área de impactos: Capacidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Espaço insuficiente para cópia Snapshot LUN (ocumEvtLunSnapshotNotPossible)	Risco	Volume	Aviso

#### Área de impactos: Configuração

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
LUN mapeado com sistema operacional não suportado no igroup(igroupUnsupportedOsType)	Risco	LUN	Aviso

#### Área de impactos: Desempenho

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Limite crítico de IOPS LUN violado (ocumLunlopsIncident)	Incidente	LUN	Crítico
Limite de aviso de IOPS LUN violado (ocumLunlopsWarning)	Risco	LUN	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
LUN MB/s limite crítico violado(ocumLunMbpsIncident)	Incidente	LUN	Crítico
Limite de aviso de MB/s LUN violado(ocumLunMbpsWarning)	Risco	LUN	Aviso
Latência de LUN ms/op limite crítico violado(ocumLunLatencyIncident)	Incidente	LUN	Crítico
Limite de aviso ms/op de latência LUN violado(ocumLunLatencyWarning)	Risco	LUN	Aviso
Latência de LUN e limite crítico de IOPS violado (ocumLunLatencyIopsIncident)	Incidente	LUN	Crítico
Limite de aviso de latência de LUN e IOPS violado (ocumLunLatencyIopsWarning)	Risco	LUN	Aviso
Latência de LUN e limite crítico de MB/s violado(ocumLunLatencyMbpsIncident)	Incidente	LUN	Crítico
Latência LUN e limite de aviso MB/s violado(ocumLunLatencyMbpsWarning)	Risco	LUN	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Latência de LUN e capacidade de desempenho agregado usada limiar crítico violado (ocumLunLatencyAggregatePerfCapacityUsedIncident)	Incidente	LUN	Crítico
Latência de LUN e capacidade de desempenho agregado usada limiar de aviso violado (ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risco	LUN	Aviso
Latência de LUN e utilização agregada limiar crítico violado(ocumLunLatencyAggregateUtilizationIncident)	Incidente	LUN	Crítico
Limite de aviso de latência de LUN e utilização de agregados violado(ocumLunLatencyAggregateUtilizationWarning)	Risco	LUN	Aviso
Latência LUN e capacidade de desempenho do nó usada limiar crítico violado (ocumLunLatencyNodePerfCapacityUsedIncident)	Incidente	LUN	Crítico
Latência LUN e capacidade de desempenho do nó usada limiar de aviso violado (ocumLunLatencyNodePerfCapacityUsedWarning)	Risco	LUN	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Latência LUN e capacidade de desempenho do nó usada - limite crítico de aquisição violado (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incidente	LUN	Crítico
Latência LUN e capacidade de desempenho do nó usada - limite de aviso de aquisição violado (ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risco	LUN	Aviso
Limite crítico de latência e utilização do nó violado (ocumLunLatencyNodeUtilizationIncident)	Incidente	LUN	Crítico
Limite de aviso de latência de LUN e utilização de nó violado(ocumLunLatencyNodeUtilizationWarning)	Risco	LUN	Aviso
Limite máximo de aviso de IOPS de LUN QoS violado (ocumQosLunMaxIopsWarning)	Risco	LUN	Aviso
QoS LUN Max MB/s limite de aviso violado(ocumQosLunMaxMbpsWarning)	Risco	LUN	Aviso
Limite de latência de LUN de carga de trabalho violado conforme definido pela Política de nível de Serviço de desempenho (ocumConformanceLatencyWarning)	Risco	LUN	Aviso



## Eventos da estação de gerenciamento

Os eventos da estação de gerenciamento fornecem informações sobre o status do servidor no qual o Unified Manager está instalado para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

### Área de impactos: Configuração

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Espaço de disco do servidor de gerenciamento quase completo (ocumEvtUnifiedManager DiskSpaceNearlyFull)	Risco	Estação de gerenciamento	Aviso
Espaço em disco do servidor de gerenciamento completo (ocumEvtUnifiedManager DiskSpaceFull)	Incidente	Estação de gerenciamento	Crítico
Servidor de gerenciamento baixo na memória (ocumEvtUnifiedManager MemoryLow)	Risco	Estação de gerenciamento	Aviso
Servidor de gerenciamento quase sem memória (ocumEvtUnifiedManager MemoryAlmostOut)	Incidente	Estação de gerenciamento	Crítico
Tamanho do arquivo de log do MySQL aumentado; reinício necessário(ocumEvtMysql LogFileSizeWarning)	Incidente	Estação de gerenciamento	Aviso
A alocação de tamanho do log de auditoria total está prestes a ficar completa	Risco	Estação de gerenciamento	Aviso
Certificado do servidor syslog prestes a expirar	Risco	Estação de gerenciamento	Aviso

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Certificado do servidor syslog expirou	Risco	Estação de gerenciamento	Erro
Ficheiro Registo Auditoria adulterado	Risco	Estação de gerenciamento	Aviso
Ficheiro de registo de auditoria eliminado	Risco	Estação de gerenciamento	Aviso
Erro de conexão do servidor syslog	Risco	Estação de gerenciamento	Erro
Configuração do servidor syslog alterada	Evento	Estação de gerenciamento	Aviso

#### Área de impactos: Desempenho

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
A análise de dados de desempenho é impactada(ocumEvtUnifiedManagerDataMissingAnalyze)	Risco	Estação de gerenciamento	Aviso
A coleta de dados de desempenho é impactada (ocumEvtUnifiedManagerDataMissCollection)	Incidente	Estação de gerenciamento	Crítico



Esses dois últimos eventos de desempenho estavam disponíveis apenas para o Unified Manager 7.2. Se algum desses eventos existir no estado novo e, em seguida, você atualizar para uma versão mais recente do software Unified Manager, os eventos não serão eliminados automaticamente. Você precisará mover os eventos para o estado resolvido manualmente.

#### Rio de Janeiro events MetroCluster

Os eventos Ponte do MetroCluster fornecem informações sobre o status das pontes para que você possa monitorar possíveis problemas em uma configuração MetroCluster sobre FC. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Ponte inalcançável (ocumEvtBridgeUnreachable)	Incidente	Ponte de MetroCluster	Crítico
Temperatura da ponte anormal (ocumEvtBridgeTemperatureAbnormal)	Incidente	Ponte de MetroCluster	Crítico

### Eventos de conectividade MetroCluster

Os eventos de conectividade fornecem informações sobre a conectividade entre os componentes de um cluster e entre clusters nas configurações MetroCluster sobre FC e MetroCluster sobre IP, para que você possa monitorar se há possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

### Eventos comuns em ambas as configurações

Esses eventos de conectividade são comuns nas configurações MetroCluster em FC e MetroCluster em IP.

### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Todos os links entre parceiros MetroCluster Down(ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Incidente	Relação de MetroCluster	Crítico
Parceiros MetroCluster não alcançáveis através da rede de peering (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Incidente	Relação de MetroCluster	Crítico
Capacidade de recuperação de desastres do MetroCluster impactada (ocumEvtMetroClusterDRStatusImpaced)	Risco	Relação de MetroCluster	Crítico

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Configuração do MetroCluster comutada (ocumEvtMetroClusterDR StatusImpated)	Risco	Relação de MetroCluster	Aviso

### Configuração de MetroCluster em FC

Esses eventos dizem respeito ao MetroCluster em configurações de FC.

### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Todos os links Inter-Switch para baixo(ocumEvtMetroClusterAllISLBetweenSwitches Down)	Incidente	Ligação entre interruptores MetroCluster	Crítico
Link de ponte FC-SAS para pilha de armazenamento para baixo(ocumEvtBridgeSas PortDown)	Incidente	Conexão de pilha de ponte MetroCluster	Crítico
Configuração do MetroCluster parcialmente comutada (ocumEvtMetroClusterDR StatusPartiallyImpated)	Risco	Relação de MetroCluster	Erro
Todos os links de interconexão FC-VI para baixo (ocumEvtMccNodeSwitch FcviLinksDown)	Incidente	Conexão do switch do nó MetroCluster	Crítico
Um ou mais links do FC-Iniciador para baixo (ocumEvtMccNodeSwitch FcLinkOneOrMoreDown)	Risco	Conexão do switch do nó MetroCluster	Aviso
Todos os links do FC-Initiator para baixo(ocumEvtMccNodeSwitchFcLinksDown)	Incidente	Conexão do switch do nó MetroCluster	Crítico

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Mudar para FC-SAS Bridge FC Link DOWN (ocumEvtMccSwitchBridgeFcLinkSWE)	Incidente	Ligação ponte do interruptor MetroCluster	Crítico
Internó todos os links de interconexão FC VI para baixo (ocumEvtMccInterNodeLinksDown)	Incidente	Conexão entre nós	Crítico
Um ou mais links de interconexão FC VI para baixo (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risco	Conexão entre nós	Aviso
Nó para Ponte Link para baixo (ocumEvtMccNodeBridgeLinkSDown)	Incidente	Conexão de ponte do nó	Crítico
Nó para pilha de armazenamento todos os links SAS para baixo (ocumEvtMccNodeStackLinkSDown)	Incidente	Conexão da pilha de nós	Crítico
Um ou mais links SAS para baixo (ocumEvtMccNodeStackLinkOneOrMoreDown)	Risco	Conexão da pilha de nós	Aviso

### Configuração MetroCluster sobre IP

Esses eventos dizem respeito às configurações MetroCluster sobre IP.

### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
O status da conectividade entre sites IP do MetroCluster está inativo (mccIntersiteconnectivityStatusDown)	Risco	Relação de MetroCluster	Crítico


Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Nó MetroCluster-IP para alternar conexão offline (mccIpPortStatusOffline)	Risco	Nó	Erro

### Eventos do switch MetroCluster

Os eventos de switch MetroCluster para configurações de MetroCluster em FC fornecem informações sobre o status dos switches MetroCluster para que você possa monitorar se há possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Interrutor de temperatura anormal (ocumEvtSwitchTemperatureAbnormal)	Incidente	Interrutor MetroCluster	Crítico
Interrutor inalcançável (ocumEvtSwitchUnreachable)	Incidente	Interrutor MetroCluster	Crítico
Falha dos ventiladores de interruptor (ocumEvtSwitchFansOneOrMoreFailed)	Incidente	Interrutor MetroCluster	Crítico
Falha nas fontes de alimentação do interruptor (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Incidente	Interrutor MetroCluster	Crítico
Falha dos sensores de temperatura do interruptor (ocumEvtSwitchTemperatureSensorFailed)	Incidente	Interrutor MetroCluster	Crítico



Este evento é aplicável apenas para switches Cisco.

## Eventos de namespace NVMe

Os eventos de namespace do NVMe fornecem informações sobre o status de seus namespaces para que você possa monitorar se há possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

Um asterisco (\*) identifica eventos EMS que foram convertidos para eventos do Unified Manager.

### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
NVMeNS Offline *(nvmeNamespaceStatusOffline)	Evento	Namespace	Informações
NVMeNS Online *(nvmeNamespaceStatusOnline)	Evento	Namespace	Informações
NVMeNS fora do espaço *(nvmeNamespaceSpaceOutOfSpace)	Risco	Namespace	Aviso
NVMeNS Destroy *(nvmeNamespaceDestroy)	Evento	Namespace	Informações

### Área de impactos: Desempenho

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Limite crítico de IOPS do NVMe violado (ocumNvmeNamespaceIopsIncident)	Incidente	Namespace	Crítico
Limite de aviso de IOPS do namespace NVMe violado (ocumNvmeNamespaceIopsWarning)	Risco	Namespace	Aviso
Limite crítico violado (ocumNvmeNamespaceMbpsIncident)	Incidente	Namespace	Crítico

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite de aviso de MB/s de NVMe violado(ocumNvmeNamespaceMbpsWarning)	Risco	Namespace	Aviso
Latência do namespace NVMe ms/op Critical Threshold violado(ocumNvmeNamespaceLatencyIncident)	Incidente	Namespace	Crítico
Limite de aviso ms/op de latência do namespace NVMe violado(ocumNvmeNamespaceLatencyWarning)	Risco	Namespace	Aviso
Latência do namespace NVMe e limite crítico de IOPS violado (ocumNvmeNamespaceLatencyIopsIncident)	Incidente	Namespace	Crítico
Latência do namespace NVMe e limite de aviso de IOPS violado (ocumNvmeNamespaceLatencyIopsWarning)	Risco	Namespace	Aviso
Latência do namespace NVMe e limite crítico de MB/s violado(ocumNvmeNamespaceLatencyMbpsIncident)	Incidente	Namespace	Crítico
Latência do namespace NVMe e limite de aviso de MB/s violado(ocumNvmeNamespaceLatencyMbpsWarning)	Risco	Namespace	Aviso

### Eventos do nó

Os eventos do nó fornecem informações sobre o status do nó para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e



incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

Um asterisco (\*) identifica eventos EMS que foram convertidos para eventos do Unified Manager.

**Área de impactos: Disponibilidade**

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Espaço de volume raiz do nó quase cheio(ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risco	Nó	Aviso
Cloud AWS MetadataConnFail *(ocumCloudAwsMetadataConnFail)	Risco	Nó	Erro
Cloud AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	Risco	Nó	Erro
Nuvem AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	Risco	Nó	Erro
Cloud AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	Risco	Nó	Erro
Cloud AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	Evento	Nó	Informações
Nuvem AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	Risco	Nó	Erro
Cloud AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	Risco	Nó	Erro

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Host de nível de nuvem não resolvível *(ocumObjstoreHostUnresolvable)	Risco	Nó	Erro
Interface de rede de Intercluster de camada de nuvem para baixo *(ocumObjstoreInterClusterLifDown)	Risco	Nó	Erro
Uma das NFSv4 piscinas esgotadas *(nbladeNfsv4PoolExhaust)	Incidente	Nó	Crítico
Assinatura do nível de nuvem de solicitação incorreta *(oscilarMismatch)	Risco	Nó	Erro

#### Área de impactos: Capacidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Memória do monitor QoS maximizada * (ocumQosMonitorMemoryMaxed)	Risco	Nó	Erro
Memória do monitor QoS abatido * (ocumQosMonitorMemoryAbated)	Evento	Nó	Informações

#### Área de impactos: Configuração

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Nó renomeado (não aplicável)	Evento	Nó	Informações

#### Área de impactos: Desempenho

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite crítico de IOPS do nó violado (ocumNodelopsIncident)	Incidente	Nó	Crítico
Limite de aviso de IOPS do nó violado (ocumNodelopsWarning)	Risco	Nó	Aviso
Limite crítico do nó MB/s violado(ocumNodeMbpsIncident)	Incidente	Nó	Crítico
Limite de aviso MB/s do nó violado(ocumNodeMbpsWarning)	Risco	Nó	Aviso
Latência do nó ms/op limite crítico violado(ocumNodeLatencyIncident)	Incidente	Nó	Crítico
Limite de aviso ms/op de latência do nó violado(ocumNodeLatencyWarning)	Risco	Nó	Aviso
Limite crítico violado (ocumNodePerfCapacityUsedIncident)	Incidente	Nó	Crítico
Limite de aviso da capacidade de desempenho do nó usado violado (ocumNodePerfCapacityUsedWarning)	Risco	Nó	Aviso
Capacidade de desempenho do nó usada - limite crítico de aquisição violado (ocumNodePerfCapacityUsedTakooverIncident)	Incidente	Nó	Crítico

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Capacidade de desempenho do nó usada - limite de aviso de aquisição violado (ocumNodePerfCapacityUsedTakeoverWarning)	Risco	Nó	Aviso
Limite crítico de utilização do nó violado (ocumNodeUtilizationIncident)	Incidente	Nó	Crítico
Limite de aviso de utilização do nó violado (ocumNodeUtilizationWarning)	Risco	Nó	Aviso
Nó HA par sobre-utilizado Threshold violado (ocumNodeHaPairOverUtilizedInformation)	Evento	Nó	Informações
Limite de fragmentação do disco do nó violado (ocumNodeDiskFragmentationWarning)	Risco	Nó	Aviso
Limite de capacidade de desempenho usado violado (ocumNodeOverUtilizedWarning)	Risco	Nó	Aviso
Limite dinâmico do nó violado (ocumNodeDynamicEventWarning)	Risco	Nó	Aviso

**Área de impactos: Segurança**

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
ID de aviso: NTAP-advisory ID>(ocumx)	Risco	Nó	Crítico

## Eventos da bateria do NVRAM

Os eventos de bateria NVRAM fornecem informações sobre o estado das suas baterias para que possa monitorizar potenciais problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Bateria de NVRAM baixa (ocumEvtNvramBatteryLow)	Risco	Nó	Aviso
NVRAM bateria descarregada (ocumEvtNvramBatteryDischarged)	Risco	Nó	Erro
NVRAM bateria excessivamente carregada (ocumEvtNvramBatteryOverCharged)	Incidente	Nó	Crítico

## Eventos portuários

Os eventos de porta fornecem status sobre as portas do cluster para que você possa monitorar alterações ou problemas na porta, como se a porta está inativa.

### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Status da porta para baixo (ocumEvtPortStatusDown)	Incidente	Nó	Crítico

### Área de impactos: Desempenho

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite crítico de MB/s da porta de rede violado(ocumNetworkPortMbpsIncident)	Incidente	Porta	Crítico
Limite de aviso da porta de rede MB/s violado(ocumNetworkPortMbpsWarning)	Risco	Porta	Aviso
Limite crítico de MB/s da porta FCP violado(ocumFcpPortMbpsIncident)	Incidente	Porta	Crítico
Limite de aviso da porta FCP MB/s violado(ocumFcpPortMbpsWarning)	Risco	Porta	Aviso
Limite crítico de utilização de porta de rede violado (ocumNetworkPortUtilizationIncident)	Incidente	Porta	Crítico
Limite de aviso de utilização de porta de rede violado(ocumNetworkPortUtilizationWarning)	Risco	Porta	Aviso
Limiar crítico de utilização de portas FCP violado (ocumFcpPortUtilizationIncident)	Incidente	Porta	Crítico
Limite de aviso de utilização de porta FCP violado(ocumFcpPortUtilizationWarning)	Risco	Porta	Aviso

### **Eventos de fontes de alimentação**

Os eventos de fontes de alimentação fornecem informações sobre o status do hardware para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Uma ou mais fontes de alimentação falhadas (ocumEvtPowerSupplyOn eOrMoreFailed)	Incidente	Nó	Crítico

#### Eventos de proteção

Os eventos de proteção informam se um trabalho falhou ou foi abortado para que você possa monitorar problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Proteção

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Falha no trabalho de proteção (ocumEvtProtectionJobTaskFailed)	Incidente	Serviço de volume ou storage	Crítico
Trabalho de proteção abortado(ocumEvtProtectionJobAborted)	Risco	Serviço de volume ou storage	Aviso

#### Eventos de Qtree

Os eventos Qtree fornecem informações sobre a capacidade de qtree e os limites de arquivo e disco para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Capacidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Qtree Space quase Full (ocumEvtQtreeSpaceNearlyFull)	Risco	Qtree	Aviso
Qtree Space Full (ocumEvtQtreeSpaceFull)	Risco	Qtree	Erro

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Qtree espaço normal (ocumEvtQtreeSpaceThresholdOk)	Evento	Qtree	Informações
Limite rígido dos arquivos Qtree atingido(ocumEvtQtreeFilesHardLimitReached)	Incidente	Qtree	Crítico
Qtree Files Soft Limit violado(ocumEvtQtreeFilesSoftLimitBreached)	Risco	Qtree	Aviso
Limite rígido do espaço de Qtree atingido(ocumEvtQtreeSpaceHardLimitReached)	Incidente	Qtree	Crítico
Qtree Space Soft Limit violado(ocumEvtQtreeSpaceSoftLimitBreached)	Risco	Qtree	Aviso

### Eventos do processador de serviço

Os eventos do processador de serviço fornecem informações sobre o status do processador para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Processador de Serviço não configurado (ocumEvtServiceProcessorNotConfigured)	Risco	Nó	Aviso
Processador de Serviço Offline (ocumEvtServiceProcessorOffline)	Risco	Nó	Erro



## Eventos de relacionamento do SnapMirror

Os eventos de relacionamento do SnapMirror fornecem informações sobre o status dos relacionamentos SnapMirror síncronos e assíncronos, para que você possa monitorar se há problemas em potencial. Os eventos de relacionamento assíncrono com o SnapMirror são gerados para VMs e volumes de storage, mas os eventos de relacionamento de SnapMirror síncronos são gerados apenas para relacionamentos de volume. Não há eventos gerados para volumes constituintes que façam parte das relações de recuperação de desastres da Storage VM. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

### Área de impactos: Proteção

Um asterisco (\*) identifica eventos EMS que foram convertidos para eventos do Unified Manager.



Os eventos de relacionamentos do SnapMirror são gerados para VMs de armazenamento protegidas pela recuperação de desastres da VM de armazenamento, mas não para quaisquer relacionamentos de objetos constituintes.

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Replicação de espelho não saudável (ocumEvtSnapmirrorRelacionamentoDessaudável)	Risco	Relação de SnapMirror	Aviso
Replicação de espelho quebrado(ocumEvtSnapmirrorRelacionamentoStateBrokenoff)	Risco	Relação de SnapMirror	Erro
Falha na inicialização da replicação do espelho(ocumEvtSnapmirrorRelationshipInitializeFailed)	Risco	Relação de SnapMirror	Erro
Falha na atualização de replicação do espelho(ocumEvtSnapmirrorRelationshipUpdateFailed)	Risco	Relação de SnapMirror	Erro
Erro de atraso de replicação do espelho (ocumEvtSnapMirrorRelationshipLagError)	Risco	Relação de SnapMirror	Erro

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Aviso de atraso de replicação do espelho (ocumEvtSnapMirrorRelationshipLagWarning)	Risco	Relação de SnapMirror	Aviso
Falha na ressincronização da replicação do espelho (ocumEvtSnapmirrorRelationshipResyncFailed)	Risco	Relação de SnapMirror	Erro
Replicação síncrona fora de sincronização *(syncSnapmirrorRelacionamentoOUTofsync)	Risco	Relação de SnapMirror	Aviso
Replicação síncrona restaurada *(syncSnapmirrorRelationshipInSync)	Evento	Relação de SnapMirror	Informações
Replicação síncrona Auto Resync falhou *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Risco	Relação de SnapMirror	Erro
O Mediador ONTAP é adicionado ao cluster (snapmirrorMediatorAdded)	Evento	Cluster	Informações
O Mediador ONTAP é removido do cluster (snapmirrorMediatorRemovado)	Evento	Cluster	Informações
O Mediador ONTAP não é acessível a partir do cluster (snapmirrorMediatorUnreachable)	Risco	Mediador	Aviso
O Mediador ONTAP não está acessível a partir do cluster (snapmirrorMediatorMisconfigurado)	Risco	Mediador	Erro

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
A conectividade do Mediador ONTAP foi restabelecida e está resynced e pronta para a sincronização ativa do SnapMirror (mirrorMediatorInQuorum)	Evento	Mediador	Informações

### Eventos de relacionamento com o Asynchronous Mirror e o Vault

Os eventos de relacionamento de espelhamento assíncrono e cofre fornecem informações sobre o status de suas relações assíncronas do SnapMirror e do Vault para que você possa monitorar possíveis problemas. Os eventos Asynchronous Mirror e Vault relation são compatíveis tanto para relacionamentos de proteção de volume quanto Storage VM. Mas apenas as relações do Vault não são suportadas para recuperação de desastres da Storage VM. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Proteção



Os eventos de relacionamentos do SnapMirror e do Vault também são gerados para VMs de armazenamento protegidas pela recuperação de desastres da VM de armazenamento, mas não para quaisquer relações de objetos constituintes.

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Espelhamento assíncrono e cofre não saudável(ocumEvtMirrorVaultRelationshipUnHealthy)	Risco	Relação de SnapMirror	Aviso
Espelhamento assíncrono e Vault quebrado-off(ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risco	Relação de SnapMirror	Erro
Falha na inicialização do espelhamento assíncrono e do Vault(ocumEvtMirrorVaultRelationshipInitializeFailed)	Risco	Relação de SnapMirror	Erro

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Falha na atualização assíncrona do espelho e do Vault(ocumEvtMirrorVaultRelationshipUpdateFailed)	Risco	Relação de SnapMirror	Erro
Erro assíncrono do espelhamento e do Vault Lag(ocumEvtMirrorVaultRelationshipLagError)	Risco	Relação de SnapMirror	Erro
Espelho assíncrono e Vault Lag Warning(ocumEvtMirrorVaultRelationshipLagWarning)	Risco	Relação de SnapMirror	Aviso
Espelhamento assíncrono e Vault Resync falhou(ocumEvtMirrorVaultRelationshipResyncFailed)	Risco	Relação de SnapMirror	Erro



O evento "update failure" (Falha na atualização do SnapMirror) é gerado pelo portal Active IQ (Config Advisor).

### Eventos de snapshot

Os eventos de snapshot fornecem informações sobre o status dos snapshots, o que permite monitorar os snapshots em busca de possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento, o nome da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Eliminação automática de instantâneos desativada (não aplicável)	Evento	Volume	Informações
Eliminação automática de instantâneos ativada (não aplicável)	Evento	Volume	Informações

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Configuração de eliminação automática de instantâneos Modificada (não aplicável)	Evento	Volume	Informações

### Eventos de relacionamento do SnapVault

Os eventos de relacionamento do SnapVault fornecem informações sobre o status de seus relacionamentos do SnapVault para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Proteção

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Não saudável do cofre assíncrono(ocumEvtSnapVaultRelationshipUnHealthy)	Risco	Relação de SnapMirror	Aviso
Asynchronous Vault Broken-off(ocumEvtSnapVaultRelationshipStateBrokenoff)	Risco	Relação de SnapMirror	Erro
Falha na inicialização do cofre assíncrono(ocumEvtSnapVaultRelationshipInitializeFailed)	Risco	Relação de SnapMirror	Erro
Falha na Atualização assíncrona do Vault(ocumEvtSnapVaultRelationshipUpdateFailed)	Risco	Relação de SnapMirror	Erro
Erro de lag do Vault assíncrono(ocumEvtSnapVaultRelationshipLagError)	Risco	Relação de SnapMirror	Erro
Aviso de lag do Vault assíncrono(ocumEvtSnapVaultRelationshipLagWarning)	Risco	Relação de SnapMirror	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Falha na ressincronização assíncrona do Vault(ocumEvtSnapvaultRelationshipResyncFailed)	Risco	Relação de SnapMirror	Erro

### Eventos de configurações de failover de storage

Os eventos de configurações de failover de armazenamento (SFO) fornecem informações sobre se o failover de armazenamento está desativado ou não configurado para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Um ou mais links para baixo (ocumEvtSfoInterconnectOneOrMoreLinkDown)	Risco	Nó	Aviso
Failover de armazenamento Desativado(ocumEvtSfoSettingsDisabled)	Risco	Nó	Erro
Failover de armazenamento não configurado (ocumEvtSfoSettingsNotConfigured)	Risco	Nó	Erro
Estado de failover de armazenamento - Takeover(ocumEvtSfoStatesTakeover)	Risco	Nó	Aviso
Estado de failover de armazenamento - reembolso parcial (ocumEvtSfoStatePartialGiveback)	Risco	Nó	Erro

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Status do nó de failover de armazenamento para baixo (ocumEvtSfoNodeStatusDown)	Risco	Nó	Erro
Possibilidade de aquisição de failover de armazenamento (ocumEvtSfoTakeoversNotPossible)	Risco	Nó	Erro

### Eventos de serviços de armazenamento

Os eventos de serviços de armazenamento fornecem informações sobre a criação e subscrição de serviços de armazenamento para que possa monitorizar potenciais problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Configuração

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Serviço de armazenamento criado (não aplicável)	Evento	Serviço de storage	Informações
Serviço de armazenamento subscrito (não aplicável)	Evento	Serviço de storage	Informações
Serviço de armazenamento cancelado (não aplicável)	Evento	Serviço de storage	Informações

#### Área de impactos: Proteção

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Exclusão inesperada da Relação do SnapMirror gerenciado EvtStorageServiceUnsupportedRelationshipDeletion	Risco	Serviço de storage	Aviso
Exclusão inesperada do volume de membro do serviço de armazenamento (ocumEvtStorageServiceUnexpectedVolumeDeletion)	Incidente	Serviço de storage	Crítico

### Eventos de prateleira de armazenamento

Os eventos do compartimento de armazenamento informam se o compartimento de armazenamento apresenta alterações anormais, para que você possa monitorar se há problemas em potencial. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Faixa de tensão anormal (ocumEvtShelfVoltageAbnormal)	Risco	Compartimento de armazenamento	Aviso
Faixa de corrente anormal (ocumEvtShelfCurrentAbnormal)	Risco	Compartimento de armazenamento	Aviso
Temperatura anormal (ocumEvtShelfTemperatureAbnormal)	Risco	Compartimento de armazenamento	Aviso

### Eventos de VM de storage

Os eventos de VM de storage (Storage Virtual Machine, também conhecido como SVM) fornecem informações sobre o status de suas VMs de storage (SVMs) para que você possa monitorar em busca de possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.



Um asterisco (\*) identifica eventos EMS que foram convertidos para eventos do Unified Manager.

**Área de impactos: Disponibilidade**

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Storage VM CIFS Service Down (ocumEvtVserverCifsServiceStatusDown)	Incidente	SVM	Crítico
Serviço SVM CIFS não configurado (não aplicável)	Evento	SVM	Informações
Tentativas de conectar compartilhamento CIFS inexistente *(nbladeCifsNoPrivShare)	Incidente	SVM	Crítico
Conflito de nomes do CIFS NetBIOS *(nbladeCifsNbNbNameConflict)	Risco	SVM	Erro
Falha na operação de cópia de sombra CIFS *(cifsShadowCopyFailure)	Risco	SVM	Erro
Muitas conexões CIFS *(nbladeCifsManyAuths)	Risco	SVM	Erro
Conexão CIFS máxima excedida * (nbladeCifsMaxOpenSameFile)	Risco	SVM	Erro
Número máximo de conexão CIFS por usuário excedido *(nbladeCifsMaxSessPerUserConn)	Risco	SVM	Erro
SVM FC/FCoE Service Down (ocumEvtVserFcServiceStatusDown)	Incidente	SVM	Crítico

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
SVM iSCSI Service Down (ocumEvtVserIscsiServiceStatusDown)	Incidente	SVM	Crítico
Storage VM NFS Service Down (ocumEvtVserverNfsServiceStatusDown)	Incidente	SVM	Crítico
Serviço SVM FC/FCoE não configurado (não aplicável)	Evento	SVM	Informações
Serviço iSCSI SVM não configurado (não aplicável)	Evento	SVM	Informações
SVM NFS Service não configurado (não aplicável)	Evento	SVM	Informações
VM de armazenamento interrompida (ocumEvtVserDown)	Risco	SVM	Aviso
Servidor AV muito ocupado para aceitar novo pedido de digitalização *(nbladeVscanConnBackPressure)	Risco	SVM	Erro
Nenhuma conexão de servidor AV para verificação de vírus *(nbladeVscanNoScannerConn)	Incidente	SVM	Crítico
Nenhum servidor AV registrado *(nbladeVscanNoRegdScanner)	Risco	SVM	Erro
Nenhuma conexão de servidor AV responsiva *(nbladeVscanConnInactive)	Evento	SVM	Informações

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Tentativa de Usuário não autorizado para AV Server *(nbladeVscanBadUserPrivAccess)	Risco	SVM	Erro
Vírus encontrado por AV Server *(nbladeVscanVirusDetected)	Risco	SVM	Erro

#### Área de impactos: Configuração

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
SVM descoberto (não aplicável)	Evento	SVM	Informações
SVM excluído(não aplicável)	Evento	Cluster	Informações
SVM renomeado (não aplicável)	Evento	SVM	Informações

#### Área de impactos: Desempenho

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Limite crítico de IOPS do SVM violado (ocumSvmIopsIncident)	Incidente	SVM	Crítico
Limite de aviso de IOPS do SVM violado (ocumSvmIopsWarning)	Risco	SVM	Aviso
SVM MB/s limite crítico violado (ocumSvmMbpsIncident)	Incidente	SVM	Crítico
Limite de aviso da SVM MB/s violado(ocumSvmMbpsWarning)	Risco	SVM	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite crítico de latência do SVM violado (ocumSvmLatencyIncident)	Incidente	SVM	Crítico
Limite de aviso de latência do SVM violado (ocumSvmLatencyWarning)	Risco	SVM	Aviso

**Área de impactos: Segurança**

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Log de auditoria Desabilitado(ocumVserverAuditLogDisabled)	Risco	SVM	Aviso
Login Banner Desabilitado(ocumVserverLoginBannerDisabled)	Risco	SVM	Aviso
SSH está usando Ciphers inseguros(ocumVserverSSHInsecure)	Risco	SVM	Aviso
Login Banner alterado(ocumVserverLoginBannerChanged)	Risco	SVM	Aviso
O monitoramento anti-ransomware da VM de armazenamento está desativado (antiRansomwareSvmStateDisabled)	Risco	SVM	Aviso
O monitoramento anti-ransomware da VM de armazenamento está ativado (modo de aprendizado) (antiRansomwareSvmStateDryrun)	Evento	SVM	Informações

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
VM de armazenamento adequado para monitorização anti-ransomware (modo de Aprendizagem) (ocumEvtSvmArwCandidate)	Evento	SVM	Informações

### Eventos de quota de utilizador e grupo

Os eventos de cota de usuário e grupo fornecem informações sobre a capacidade da cota de usuário e grupo de usuários, bem como os limites de arquivo e disco para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

#### Área de impactos: Capacidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Limite de espaço em disco de quota de usuário ou grupo violado(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risco	Quota de utilizador ou grupo	Aviso
Limite rígido de espaço em disco de quota de utilizador ou de grupo atingido(ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Incidente	Quota de utilizador ou grupo	Crítico
Limite de arquivos de cota de usuário ou grupo violado(ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Risco	Quota de utilizador ou grupo	Aviso
Limite rígido de contagem de ficheiros de quota de utilizador ou grupo atingido(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Incidente	Quota de utilizador ou grupo	Crítico

## Eventos de volume

Os eventos de volume fornecem informações sobre o status dos volumes, o que permite monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento, o nome da armadilha, o nível de impactos, o tipo de origem e a gravidade.

Um asterisco (\*) identifica eventos EMS que foram convertidos para eventos do Unified Manager.

### Área de impactos: Disponibilidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Volume restrito (ocumEvtVolumeRestricted)	Risco	Volume	Aviso
Volume off-line (ocumEvtVolumeOffline)	Incidente	Volume	Crítico
Volume parcialmente disponível (ocumEvtVolumePartiallyDisponível)	Risco	Volume	Erro
Volume não montado (não aplicável)	Evento	Volume	Informações
Volume montado (não aplicável)	Evento	Volume	Informações
Volume remontado (não aplicável)	Evento	Volume	Informações
Caminho de junção de volume inativo(ocumEvtVolumeJunctionPathInactive)	Risco	Volume	Aviso
Volume Autosize ativado (não aplicável)	Evento	Volume	Informações
Volume Autosize-Disabled (tamanho automático do volume) (não aplicável)	Evento	Volume	Informações

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Volume Autosize capacidade máxima Modificada (não aplicável)	Evento	Volume	Informações
Volume Autosize Increment tamanho modificado (não aplicável)	Evento	Volume	Informações

#### Área de impactos: Capacidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Espaço em volume provisionado por thin em risco (ocumThinProvenVolumeSpaceAtRisk)	Risco	Volume	Aviso
Erro de operação de eficiência de volume (ocumEvtVolumeEfficienciaOperationError)	Risco	Volume	Erro
Volume espaço cheio (ocumEvtVolumeFull)	Risco	Volume	Erro
Volume espaço quase cheio (ocumEvtVolumeNearlyFull)	Risco	Volume	Aviso
Volume espaço lógico completo * (volumeLogicalSpaceFull)	Risco	Volume	Erro
Volume espaço lógico quase completo * (volumeLogicalSpaceNearlyFull)	Risco	Volume	Aviso
Volume espaço lógico normal *(volumeLogicalSpaceAllOK)	Evento	Volume	Informações

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Volume Snapshot Reserve Space Full(ocumEvtSnapshotFull)	Risco	Volume	Aviso
Demasiadas cópias Snapshot (ocumEvtSnapshotTooMany)	Risco	Volume	Erro
Volume Qtree quota overcommitted (ocumEvtVolumeQtreeQuotaOvercommitted)	Risco	Volume	Erro
Volume Qtree quota quase sobrecomprometida (ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Risco	Volume	Aviso
Taxa de crescimento de volume anormal (ocumEvtVolumeGrowthRateAbnormal)	Risco	Volume	Aviso
Volume dias até completo (ocumEvtVolumeDaysUntilFullSoon)	Risco	Volume	Erro
Garantia de espaço de volume desativada (não aplicável)	Evento	Volume	Informações
Garantia de espaço de volume ativada (não aplicável)	Evento	Volume	Informações
Garantia de espaço de volume modificada (não aplicável)	Evento	Volume	Informações
Volume Snapshot Reserve dias até cheio(ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risco	Volume	Erro



<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Os eleitores do FlexGroup têm questões espaciais *(flexGroupConstituentsHaveSpaceIssues)	Risco	Volume	Erro
FlexGroup constituintes Estado do espaço tudo OK *(flexGroupConstituentsSpaceStatusAll OK)	Evento	Volume	Informações
Os constituintes do FlexGroup têm inodes issues *(flexGroupConstituentsHaveNodesIssues)	Risco	Volume	Erro
FlexGroup constituintes inodes Status tudo OK *(flexGroupConstituentsInodesStatusAllOK)	Evento	Volume	Informações
WAFV volume AutoSize Fail * (wafVolAutoSizeFail)	Risco	Volume	Erro
WAFV volume AutoSize Done * (wafVolAutoSizeDone)	Evento	Volume	Informações
O volume FlexGroup é mais de 80% utilizado*	Incidente	Volume	Erro
O volume FlexGroup é mais de 90% utilizado*	Incidente	Volume	Crítico
Anomalia de eficiência de storage de volume (ocumVolumeAbnormalStorageEfficiencyWarning)	Risco	Volume	Aviso
Reserva de snapshot de volume subutilizada (volumeSnapshotReserveUnderutilizedWarning)	Evento	Volume	Aviso

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Reserva de snapshot de volume subutilizada (volumeSnapshotReserveUnderutilised)	Evento	Volume	Aviso

#### Área de impactos: Configuração

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Volume renomeado (não aplicável)	Evento	Volume	Informações
Volume descoberto (não aplicável)	Evento	Volume	Informações
Volume eliminado (não aplicável)	Evento	Volume	Informações

#### Área de impactos: Desempenho

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Limite de aviso de IOPS máximo de volume de QoS violado (ocumQosVolumeMaxIopsWarning)	Risco	Volume	Aviso
Limite máximo de aviso de MB/s de volume QoS violado (ocumQosVolumeMaxMbpsWarning)	Risco	Volume	Aviso
Limite máximo de aviso de IOPS/TB de volume QoS violado (ocumQosVolumeMaxIopsPerTbWarning)	Risco	Volume	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite de latência de volume de carga de trabalho violado conforme definido pela Política de nível de Serviço de desempenho (ocumConformanceLatencyWarning)	Risco	Volume	Aviso
Limite crítico de IOPS de volume violado (ocumVolumelopsIncident)	Incidente	Volume	Crítico
Limite de aviso de IOPS de volume violado (ocumVolumelopsWarning)	Risco	Volume	Aviso
Volume MB/s limite crítico violado(ocumVolumeMbpsIncidente)	Incidente	Volume	Crítico
Volume MB/s limiar de aviso violado(ocumVolumeMbpsWarning)	Risco	Volume	Aviso
Limite crítico de latência de volume violado (ocumVolumeLatencyIncident)	Incidente	Volume	Crítico
Limite de aviso de latência de volume violado (ocumVolumeLatencyWarning)	Risco	Volume	Aviso
Limiar crítico de perda de cache de volume violado (ocumVolumeCacheMissRatioIncident)	Incidente	Volume	Crítico

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite de aviso de taxa de perda de volume violado(ocumVolumeCacheMissRatioWarning)	Risco	Volume	Aviso
Latência de volume e limite crítico de IOPS violado (ocumVolumeLatencyIops Incident)	Incidente	Volume	Crítico
Limite de aviso de latência de volume e IOPS violado (ocumVolumeLatencyIops Warning)	Risco	Volume	Aviso
Latência de volume e limite crítico de MB/s violado(ocumVolumeLatencyMbpsIncident)	Incidente	Volume	Crítico
Latência de volume e limite de aviso de MB/s violado(ocumVolumeLatencyMbpsWarning)	Risco	Volume	Aviso
Latência de volume e capacidade de desempenho agregado usada limiar crítico violado (ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Incidente	Volume	Crítico
Latência de volume e capacidade de desempenho agregado usada limiar de aviso violado (ocumVolumeLatencyAggregatePerfCapacityUsed Warning)	Risco	Volume	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Latência de volume e utilização agregada limiar crítico violado (ocumVolumeLatencyAggregateUtilizationIncident)	Incidente	Volume	Crítico
Limite de aviso de latência de volume e utilização agregada violado (ocumVolumeLatencyAggregateUtilizationWarning)	Risco	Volume	Aviso
Latência de volume e capacidade de desempenho do nó usada limiar crítico violado (ocumVolumeLatencyNodePerfCapacityUsedIncident)	Incidente	Volume	Crítico
Latência de volume e capacidade de desempenho do nó usada limiar de aviso violado (ocumVolumeLatencyNodePerfCapacityUsedWarning)	Risco	Volume	Aviso
Latência de volume e capacidade de desempenho do nó usada - limite crítico de aquisição violado (ocumVolumeLatencyAggregatePerfCapacityUsedTakeOverIncident)	Incidente	Volume	Crítico
Latência de volume e capacidade de desempenho do nó usada - limite de aviso de aquisição violado (ocumVolumeLatencyAggregatePerfCapacityUsedTakeOverWarning)	Risco	Volume	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
Limite crítico de latência e utilização de nó violado (ocumVolumeLatencyNodeUtilizationIncident)	Incidente	Volume	Crítico
Limite de aviso de latência de volume e utilização de nó violado (ocumVolumeLatencyNodeUtilizationWarning)	Risco	Volume	Aviso

**Área de impactos: Segurança**

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
O monitoramento anti-ransomware de volume está ativado (modo Ativo) (antiRansomwareVolumeStateEnabled)	Evento	Volume	Informações
O monitoramento anti-ransomware de volume está desativado (antiRansomwareVolumeStatesDisabled)	Risco	Volume	Aviso
O monitoramento anti-ransomware de volume está ativado (modo de Aprendizagem) (antiRansomwareVolumeStateDryrun)	Evento	Volume	Informações
O monitoramento de volume anti-ransomware é pausado (modo de Aprendizagem) (antiRansomwareVolumeStateDryrunPaused)	Risco	Volume	Aviso
O monitoramento de volume anti-ransomware é pausado (modo Ativo) (antiRansomwareVolumeStateEnablePaused)	Risco	Volume	Aviso

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
O monitoramento anti-ransomware de volume está desabilitado (antiRansomwareVolumeStatesDisableInProgress)	Risco	Volume	Aviso
Atividade de ransomware vista (callHomeRansomwareActivitySeen)	Incidente	Volume	Crítico
Volume adequado para monitorização anti-ransomware (modo de Aprendizagem) (ocumEvtVolumeArwCandidate)	Evento	Volume	Informações
Volume adequado para monitoramento anti-ransomware (modo Ativo) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Risco	Volume	Aviso
Volume exibe um alerta anti-ransomware ruidoso (antiRansomwareFeatureNoisyvolume)	Risco	Volume	Aviso

#### Área de impactos: Proteção de dados

<b>Nome do evento (Nome da armadilha)</b>	<b>Nível de impactos</b>	<b>Tipo de origem</b>	<b>Gravidade</b>
O volume não tem proteção local Snapshot (VolumeLacksLocalProtectionWarning)	Risco	Volume	Aviso
O volume não tem proteção local Snapshot (VolumeLacksLocalProtectionCleared)	Risco	Volume	Aviso

## Eventos de status de movimentação de volume

Os eventos de status de movimentação de volume informam sobre o status da movimentação de volume para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impactos e incluem o nome do evento e da armadilha, o nível de impactos, o tipo de origem e a gravidade.

### Área de impactos: Capacidade

Nome do evento (Nome da armadilha)	Nível de impactos	Tipo de origem	Gravidade
Status de movimentação de volume: Em andamento (não aplicável)	Evento	Volume	Informações
Estado de movimentação de volume - falhou(ocumEvtVolumeMoveFailed)	Risco	Volume	Erro
Status de movimentação de volume: Concluído (não aplicável)	Evento	Volume	Informações
Movimentação de volume - redução diferida (ocumEvtVolumeMoveCutoverDeferido)	Risco	Volume	Aviso

## Descrição das janelas de eventos e caixas de diálogo

Eventos notificá-lo sobre quaisquer problemas em seu ambiente. Você pode usar a página de inventário de Gerenciamento de Eventos e a página de detalhes do evento para monitorar todos os eventos. Você pode usar a caixa de diálogo Opções de configuração de notificação para configurar a notificação. Pode utilizar a página Configuração de eventos para desativar ou ativar eventos.

### Página de notificações

Você pode configurar o servidor do Unified Manager para enviar notificações quando um evento é gerado ou quando ele é atribuído a um usuário. Você também pode configurar os mecanismos de notificação. Por exemplo, as notificações podem ser enviadas como e-mails ou traps SNMP.

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



## E-mail

Esta área permite configurar as seguintes definições de e-mail para notificação de alerta:

- **De Endereço**

Especifica o endereço de e-mail a partir do qual a notificação de alerta é enviada. Esse valor também é usado como endereço de para um relatório quando compartilhado. Se o Endereço de for preenchido com o endereço "[ActiveQUnifiedManager@localhost.com](mailto:ActiveQUnifiedManager@localhost.com)", você deve alterá-lo para um endereço de e-mail real e funcional para garantir que todas as notificações de e-mail sejam entregues com sucesso.

## SMTP Server

Esta área permite configurar as seguintes definições do servidor SMTP:

- **Nome do host ou endereço IP**

Especifica o nome do host do servidor host SMTP, que é usado para enviar a notificação de alerta para os destinatários especificados.

- **Nome de usuário**

Especifica o nome de usuário SMTP. O nome de usuário SMTP só é necessário quando o SMTPAUTH está habilitado no servidor SMTP.

- **Senha**

Especifica a senha SMTP. O nome de usuário SMTP só é necessário quando o SMTPAUTH está habilitado no servidor SMTP.

- **Porto**

Especifica a porta que é usada pelo servidor host SMTP para enviar notificação de alerta.

O valor padrão é 25.

- **Use START/TLS**

Marcar esta caixa fornece comunicação segura entre o servidor SMTP e o servidor de gerenciamento usando os protocolos TLS/SSL (também conhecidos como start\_TLS e STARTTLS).

- **Use SSL**

Marcar esta caixa fornece comunicação segura entre o servidor SMTP e o servidor de gerenciamento usando o protocolo SSL.

## SNMP

Esta área permite configurar as seguintes definições de trap SNMP:

- **Versão**

Especifica a versão SNMP que você deseja usar dependendo do tipo de segurança que você precisa. As opções incluem a versão 1, a versão 3, a versão 3 com autenticação e a versão 3 com autenticação e encriptação. O valor padrão é a versão 1.

- **Trap Destination Host**

Especifica o nome do host ou o endereço IP (IPv4 ou IPv6) que recebe os traps SNMP enviados pelo servidor de gerenciamento. Para especificar vários destinos de intercetação, separe cada host com uma vírgula.



Todas as outras configurações SNMP, como "versão" e "porta de saída", devem ser as mesmas para todos os hosts da lista.

- **\* Outbound Trap Port\***

Especifica a porta através da qual o servidor SNMP recebe os traps que são enviados pelo servidor de gerenciamento.

O valor padrão é 162.

- **Comunidade**

A string da comunidade para acessar o host.

- **ID do motor**

Especifica o identificador exclusivo do agente SNMP e é gerado automaticamente pelo servidor de gerenciamento. A ID do motor está disponível com SNMP versão 3, SNMP versão 3 com autenticação e SNMP versão 3 com autenticação e encriptação.

- **Nome de usuário**

Especifica o nome de usuário SNMP. O nome de utilizador está disponível com SNMP versão 3, SNMP versão 3 com autenticação e SNMP versão 3 com autenticação e encriptação.

- **Protocolo de autenticação**

Especifica o protocolo usado para autenticar um usuário. As opções de protocolo incluem MD5 e SHA. MD5 é o valor padrão. O protocolo de autenticação está disponível com SNMP versão 3 com Autenticação e SNMP versão 3 com Autenticação e encriptação.

- **Senha de autenticação**

Especifica a senha usada ao autenticar um usuário. A palavra-passe de autenticação está disponível com SNMP versão 3 com Autenticação e SNMP versão 3 com Autenticação e encriptação.

- **Protocolo de Privacidade**

Especifica o protocolo de privacidade usado para criptografar mensagens SNMP. As opções de protocolo incluem AES 128 e DES. O valor padrão é AES 128. O protocolo de privacidade está disponível com o SNMP versão 3 com Autenticação e criptografia.

- **Senha de privacidade**

Especifica a senha ao usar o protocolo de privacidade. A palavra-passe de privacidade está disponível com SNMP versão 3 com Autenticação e encriptação.

Para obter mais informações sobre objetos e traps SNMP, você pode baixar o ["MIB Active IQ Unified Manager"](#) no site de suporte da NetApp.

## Página de inventário do Gerenciamento de Eventos

A página de inventário de Gerenciamento de Eventos permite exibir uma lista de eventos atuais e suas propriedades. Você pode executar tarefas como reconhecer, resolver e atribuir eventos. Você também pode adicionar um alerta para eventos específicos.

As informações nesta página são atualizadas automaticamente a cada 5 minutos para garantir que os novos eventos mais atuais sejam exibidos.

### Componentes do filtro

Permite-lhe personalizar as informações apresentadas na lista de eventos. Você pode refinar a lista de eventos que são exibidos usando os seguintes componentes:

- Menu View (Ver) para selecionar a partir de uma lista predefinida de seleções de filtros.

Isso inclui itens como todos os eventos ativos (novos e reconhecidos), eventos de desempenho ativo, eventos atribuídos a mim (o usuário conectado) e todos os eventos gerados durante todas as janelas de manutenção.

- Painel de pesquisa para refinar a lista de eventos inserindo termos completos ou parciais.
- Botão de filtro que inicia o painel filtros para que você possa selecionar a partir de cada campo e atributo de campo disponível para refinar a lista de eventos.

### Botões de comando

Os botões de comando permitem executar as seguintes tarefas:

- **Atribuir a**

Permite-lhe selecionar o utilizador a quem o evento é atribuído. Quando você atribui um evento a um usuário, o nome de usuário e a hora em que o evento foi atribuído são adicionados na lista de eventos para os eventos selecionados.

- Eu

Atribui o evento ao usuário conectado atualmente.

- Outro utilizador

Exibe a caixa de diálogo atribuir proprietário, que permite atribuir ou reatribuir o evento a outros usuários. Você também pode cancelar a atribuição de eventos deixando o campo propriedade em branco.

- **Reconhecimento**

Reconhece os eventos selecionados.

Quando você reconhece um evento, seu nome de usuário e a hora em que você reconheceu o evento são adicionados na lista de eventos para os eventos selecionados. Quando você reconhece um evento, você é responsável por gerenciar esse evento.



Você não pode reconhecer eventos de informações.

- **Marcar como resolvido**

Permite alterar o estado do evento para resolvido.

Quando você resolve um evento, seu nome de usuário e a hora em que você resolveu o evento são adicionados na lista de eventos para os eventos selecionados. Depois de tomar medidas corretivas para o evento, você deve marcar o evento como resolvido.

- **Adicionar alerta**

Exibe a caixa de diálogo Adicionar alerta, que permite adicionar alertas para os eventos selecionados.

- **Relatórios**

Permite exportar detalhes da exibição de evento atual para um arquivo de valores separados por vírgulas (.csv) ou documento PDF.

- **Mostrar/Ocultar Seletor de coluna**

Permite-lhe escolher as colunas que são apresentadas na página e selecionar a ordem em que são apresentadas.

## Lista de eventos

Exibe detalhes de todos os eventos ordenados por hora acionada.

Por padrão, a exibição todos os eventos ativos é exibida para mostrar os eventos novos e reconhecidos dos sete dias anteriores que têm um nível de impactos de Incidente ou risco.

- **Tempo acionado**

O momento em que o evento foi gerado.

- **Gravidade**

Gravidade do evento: Crítica (❌), erro (⚠️), Aviso (⚠️) e informações (ℹ️).

- **Estado**

O estado do evento: Novo, reconhecido, resolvido ou Obsoleto.

- **Nível de impactos**

O nível de impacto do evento: Incidente, risco, evento ou upgrade.

- **Área de impactos**

A área de impacto de eventos: Disponibilidade, capacidade, desempenho, proteção, configuração ou segurança.

- **Nome**

O nome do evento. Você pode selecionar o nome para exibir a página de detalhes do evento para esse evento.

- **Fonte**

O nome do objeto no qual o evento ocorreu. Você pode selecionar o nome para exibir a página de detalhes de integridade ou desempenho para esse objeto.

Quando ocorre uma violação de política de QoS compartilhada, somente o objeto de workload que está consumindo a maioria das IOPS ou MB/s é mostrado neste campo. Cargas de trabalho adicionais que estão usando esta política são exibidas na página de detalhes do evento.

- **Tipo de fonte**

O tipo de objeto (por exemplo, Storage VM, volume ou Qtree) com o qual o evento está associado.

- **Atribuído a**

O nome do usuário ao qual o evento é atribuído.

- **Origem do evento**

Se o evento teve origem no "Portal Active IQ" ou diretamente do "Active IQ Unified Manager".

- **Nome da anotação**

O nome da anotação atribuída ao objeto de armazenamento.

- **Notas**

O número de notas que são adicionadas para um evento.

- **Dias pendentes**

O número de dias desde o evento foi inicialmente gerado.

- **Hora atribuída**

O tempo decorrido desde que o evento foi atribuído a um usuário. Se o tempo decorrido exceder uma semana, o carimbo de data/hora quando o evento foi atribuído a um usuário é exibido.

- **Reconhecido por**

O nome do usuário que reconheceu o evento. O campo fica em branco se o evento não for reconhecido.

- **Hora reconhecida**

O tempo decorrido desde que o evento foi reconhecido. Se o tempo decorrido exceder uma semana, é apresentado o carimbo de data/hora quando o evento foi reconhecido.

- **Resolvido por**

O nome do usuário que resolveu o evento. O campo fica em branco se o evento não for resolvido.

- **Tempo resolvido**

O tempo decorrido desde que o evento foi resolvido. Se o tempo decorrido exceder uma semana, o carimbo de data/hora quando o evento foi resolvido é exibido.

- **Tempo obsoleto**

A época em que o estado do evento se tornou Obsoleto.

## **Página de detalhes do evento**

Na página de detalhes do evento, você pode exibir os detalhes de um evento selecionado, como a gravidade do evento, o nível de impactos, a área de impactos e a origem do evento. Você também pode exibir informações adicionais sobre possíveis correções para resolver o problema.

- **Nome do evento**

O nome do evento e a hora em que o evento foi visto pela última vez.

Para eventos que não sejam de desempenho, enquanto o evento estiver no estado novo ou reconhecido, a última informação vista não é conhecida e, portanto, está oculta.

- **Descrição do evento**

Uma breve descrição do evento.

Em alguns casos, um motivo para o evento ser acionado é fornecido na descrição do evento.

- **Componente em contenção**

Para eventos de desempenho dinâmico, esta seção exibe ícones que representam os componentes lógicos e físicos do cluster. Se um componente estiver na contenção, seu ícone será circulado e destacado em vermelho.

Consulte *componentes de cluster e por que eles podem estar na contenção* para obter uma descrição dos componentes que são exibidos aqui.

As seções informações de eventos, Diagnóstico do sistema e ações sugeridas são descritas em outros tópicos.

## **Botões de comando**

Os botões de comando permitem executar as seguintes tarefas:

- **Ícone de notas**

Permite adicionar ou atualizar uma nota sobre o evento e rever todas as notas deixadas por outros utilizadores.

## **Menu ações**

- **Atribuir a mim**

Atribui o evento a você.

- **Atribuir a outros**

Abre a caixa de diálogo atribuir proprietário, que permite atribuir ou reatribuir o evento a outros usuários.

Quando você atribui um evento a um usuário, o nome do usuário e a hora em que o evento foi atribuído são adicionados na lista de eventos para os eventos selecionados.

Você também pode cancelar a atribuição de eventos deixando o campo propriedade em branco.

- **Reconhecimento**

Reconhece os eventos selecionados para que não continue a receber notificações de alerta repetidas.

Quando você reconhece um evento, seu nome de usuário e a hora em que você reconheceu o evento são adicionados na lista de eventos (reconhecidos por) para os eventos selecionados. Quando você reconhece um evento, você assume a responsabilidade de gerenciar esse evento.

- **Marcar como resolvido**

Permite alterar o estado do evento para resolvido.

Quando você resolve um evento, seu nome de usuário e a hora em que você resolveu o evento são adicionados na lista de eventos (resolvidos por) para os eventos selecionados. Depois de tomar medidas corretivas para o evento, você deve marcar o evento como resolvido.

- **Adicionar alerta**

Exibe a caixa de diálogo Adicionar alerta, que permite adicionar um alerta para o evento selecionado.

#### O que a seção informações do evento exibe

Você usa a seção informações do evento na página de detalhes do evento para exibir os detalhes sobre um evento selecionado, como a gravidade do evento, o nível de impactos, a área de impactos e a origem do evento.

Os campos que não são aplicáveis ao tipo de evento estão ocultos. Você pode ver os seguintes detalhes do evento:

- **Tempo de ativação do evento**

O momento em que o evento foi gerado.

- **Estado**

O estado do evento: Novo, reconhecido, resolvido ou Obsoleto.

- **Causa obsoleta**

As ações que fizeram com que o evento fosse obsoleto, por exemplo, o problema foi corrigido.

- **Duração do evento**

Para eventos ativos (novos e reconhecidos), este é o tempo entre a detecção e o momento em que o evento foi analisado pela última vez. Para eventos obsoletos, este é o tempo entre a detecção e quando o evento foi resolvido.

Este campo é exibido para todos os eventos de desempenho e para outros tipos de eventos somente


depois que eles tiverem sido resolvidos ou obsoletos.

- **Último visto**

A data e hora em que o evento foi visto pela última vez como ativo.

Para eventos de desempenho, este valor pode ser mais recente do que o tempo de disparo do evento, uma vez que este campo é atualizado após cada nova recolha de dados de desempenho, desde que o evento esteja ativo. Para outros tipos de eventos, quando no estado novo ou reconhecido, este conteúdo não é atualizado e o campo fica, portanto, oculto.

- **Gravidade**

Gravidade do evento: Crítica () , erro () , Aviso () e informações () .

- **Nível de impactos**

O nível de impacto do evento: Incidente, risco, evento ou upgrade.

- **Área de impactos**

A área de impacto de eventos: Disponibilidade, capacidade, desempenho, proteção, configuração ou segurança.

- **Fonte**

O nome do objeto no qual o evento ocorreu.

Ao exibir os detalhes de um evento de política de QoS compartilhada, até três dos objetos de workload que estão consumindo a maioria das IOPS ou Mbps são listados neste campo.

Você pode clicar no link do nome da fonte para exibir a página de detalhes de integridade ou desempenho desse objeto.

- **Anotações de origem**

Apresenta o nome e o valor da anotação para o objeto ao qual o evento está associado.

Esse campo é exibido apenas para eventos de integridade em clusters, SVMs e volumes.

- **Grupos de origem**

Exibe os nomes de todos os grupos dos quais o objeto impactado é membro.

Esse campo é exibido apenas para eventos de integridade em clusters, SVMs e volumes.

- **Tipo de fonte**

O tipo de objeto (por exemplo, SVM, volume ou Qtree) ao qual o evento está associado.

- **No Cluster**

O nome do cluster no qual o evento ocorreu.

Você pode clicar no link do nome do cluster para exibir a página de detalhes de integridade ou desempenho desse cluster.



- **Contagem de objetos afetados**

O número de objetos afetados pelo evento.

Você pode clicar no link objeto para exibir a página de inventário preenchida com os objetos que estão atualmente afetados por este evento.

Este campo é exibido apenas para eventos de desempenho.

- **Volumes afetados**

O número de volumes que estão sendo afetados por este evento.

Este campo é exibido apenas para eventos de desempenho em nós ou agregados.

- **Política acionada**

O nome da política de limite que emitiu o evento.

Você pode passar o cursor sobre o nome da política para ver os detalhes da política de limite. Para políticas de QoS adaptáveis, a política definida, o tamanho do bloco e o tipo de alocação (espaço alocado ou espaço usado) também são exibidos.

Este campo é exibido apenas para eventos de desempenho.

- **ID da regra**

Para eventos da plataforma Active IQ, esse é o número da regra que foi acionada para gerar o evento.

- **Reconhecido por**

O nome da pessoa que reconheceu o evento e a hora em que o evento foi reconhecido.

- **Resolvido por**

O nome da pessoa que resolveu o evento e a hora em que o evento foi resolvido.

- **Atribuído a**

O nome da pessoa que está designada para trabalhar no evento.

- **Configurações de alerta**

As seguintes informações sobre alertas são exibidas:

- Se não houver alertas associados ao evento selecionado, um link **Adicionar alerta** será exibido.

Você pode abrir a caixa de diálogo Adicionar alerta clicando no link.

- Se houver um alerta associado ao evento selecionado, o nome do alerta será exibido.

Você pode abrir a caixa de diálogo Editar alerta clicando no link.

- Se houver mais de um alerta associado ao evento selecionado, o número de alertas será exibido.

Você pode abrir a página Configuração de alertas clicando no link para ver mais detalhes sobre esses

alertas.

Os alertas desativados não são exibidos.

- **Última notificação enviada**

A data e hora em que a notificação de alerta mais recente foi enviada.

- **Enviar por**

O mecanismo que foi usado para enviar a notificação de alerta: Email ou intercetação SNMP.

- \* Execução de Script anterior\*

O nome do script que foi executado quando o alerta foi gerado.

#### O que a seção ações sugeridas é exibida

A seção ações sugeridas da página de detalhes do evento fornece possíveis razões para o evento e sugere algumas ações para que você possa tentar resolver o evento por conta própria. As ações sugeridas são personalizadas com base no tipo de evento ou tipo de limite que foi violado.

Esta área é apresentada apenas para alguns tipos de eventos.

Em alguns casos, há links **Ajuda** fornecidos na página que fazem referência a informações adicionais para muitas ações sugeridas, incluindo instruções para executar uma ação específica. Algumas das ações podem envolver o uso dos comandos do Unified Manager, do ONTAP System Manager, do OnCommand Workflow Automation, da CLI do ONTAP ou uma combinação dessas ferramentas.

Você deve considerar as ações sugeridas aqui como apenas uma orientação para resolver este evento. A ação que você toma para resolver este evento deve ser baseada no contexto do seu ambiente.

Se você quiser analisar o objeto e o evento com mais detalhes, clique no botão **Analyze Workload** para exibir a página análise de carga de trabalho.

Há certos eventos que o Unified Manager pode diagnosticar cuidadosamente e fornecer uma única resolução. Quando disponíveis, essas resoluções são exibidas com um botão **Fix it**. Clique neste botão para que o Unified Manager corrija o problema que causa o evento.

Para eventos da plataforma Active IQ, esta seção pode conter um link para um artigo da base de conhecimento do NetApp, quando disponível, que descreve o problema e possíveis resoluções. Em sites sem acesso à rede externa, um PDF do artigo da base de conhecimento é aberto localmente; o PDF faz parte do arquivo de regras que você baixa manualmente para a instância do Unified Manager.

#### O que é apresentado na seção Diagnóstico do sistema

A seção Diagnóstico do sistema da página de detalhes do evento fornece informações que podem ajudá-lo a diagnosticar problemas que possam ter sido responsáveis pelo evento.

Esta área é apresentada apenas para alguns eventos.

Alguns eventos de desempenho fornecem gráficos que são relevantes para o evento específico que foi

acionado. Normalmente, isso inclui um gráfico de IOPS ou Mbps e um gráfico de latência para os dez dias anteriores. Quando organizado dessa maneira, você pode ver quais componentes de storage estão afetando a latência ou sendo afetados pela latência, quando o evento está ativo.

Para eventos de desempenho dinâmico, os seguintes gráficos são exibidos:

- Latência da carga de trabalho - exibe o histórico de latência das principais cargas de trabalho de vítima, agressor ou tubarão no componente em disputa.
- Atividade do workload - exibe detalhes sobre o uso do workload do componente do cluster na contenção.
- Atividade de recurso - exibe estatísticas históricas de desempenho para o componente de cluster em contenção.

Outros gráficos são exibidos quando alguns componentes de cluster estão em contenção.

Outros eventos fornecem uma breve descrição do tipo de análise que o sistema está executando no objeto de armazenamento. Em alguns casos, haverá uma ou mais linhas; uma para cada componente analisado, para políticas de desempenho definidas pelo sistema que analisam vários contadores de desempenho. Neste cenário, é apresentado um ícone verde ou vermelho junto ao diagnóstico para indicar se foi ou não encontrado um problema nesse diagnóstico específico.

### **Página Configuração do evento**

A página Configuração do evento exibe a lista de eventos desativados e fornece informações como o tipo de objeto associado e a gravidade do evento. Você também pode executar tarefas como desabilitar ou habilitar eventos globalmente.

Você só pode acessar esta página se tiver a função Administrador de aplicativos ou Administrador de armazenamento.

#### **Botões de comando**

Os botões de comando permitem executar as seguintes tarefas para eventos selecionados:

- **Desativar**

Inicia a caixa de diálogo Desativar eventos, que pode ser utilizada para desativar eventos.

- **Ativar**

Ativa eventos selecionados que você escolheu para desativar anteriormente.

- **Regras de upload**

Inicia a caixa de diálogo regras de carregamento, que permite que sites sem acesso à rede externa carreguem manualmente o arquivo de regras do Active IQ para o Gerenciador Unificado. As regras são executadas em mensagens do cluster AutoSupport para gerar eventos para configuração do sistema, cabeamento, práticas recomendadas e disponibilidade, conforme definido pela plataforma Active IQ.

- **Subscribe to EMS Events**

Inicia a caixa de diálogo assinar eventos EMS, que permite que você se inscreva para receber eventos específicos do sistema de gerenciamento de eventos (EMS) dos clusters que você está monitorando. O EMS recolhe informações sobre eventos que ocorrem no cluster. Quando uma notificação é recebida para um evento EMS subscrito, um evento do Unified Manager é gerado com a gravidade apropriada.

## Vista de lista

O modo de exibição Lista exibe informações (em formato tabular) sobre eventos desativados. Você pode usar os filtros de coluna para personalizar os dados exibidos.

- **Evento**

Exibe o nome do evento que está desativado.

- **Gravidade**

Exibe a gravidade do evento. A gravidade pode ser Crítica, erro, Aviso ou Informação.

- **Tipo de fonte**

Exibe o tipo de origem para o qual o evento é gerado.

## Caixa de diálogo Desativar eventos

A caixa de diálogo Desativar eventos exibe a lista de tipos de eventos para os quais você pode desativar eventos. Você pode desativar eventos para um tipo de evento com base em uma gravidade específica ou em um conjunto de eventos.

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

### Área Propriedades do evento

A área Propriedades do evento especifica as seguintes propriedades do evento:

- **Gravidade do evento**

Permite selecionar eventos com base no tipo de gravidade, que pode ser Crítica, erro, Aviso ou Informação.

- **Nome do evento contém**

Permite filtrar eventos cujo nome contém os caracteres especificados.

- **Eventos correspondentes**

Exibe a lista de eventos que correspondem ao tipo de gravidade do evento e à cadeia de texto especificada.

- **Desativar eventos**

Exibe a lista de eventos que você selecionou para desativar.

A gravidade do evento também é exibida juntamente com o nome do evento.

### Botões de comando

Os botões de comando permitem executar as seguintes tarefas para os eventos selecionados:

- **Salvar e fechar**

Desativa o tipo de evento e fecha a caixa de diálogo.

- **Cancelar**

Descarta as alterações e fecha a caixa de diálogo.

## Gerenciamento de alertas

Você pode configurar alertas para enviar notificações automaticamente quando eventos ou eventos específicos de determinados tipos de gravidade ocorrerem. Você também pode associar um alerta a um script que é executado quando um alerta é acionado.

### Quais são os alertas

Embora os eventos ocorram continuamente, o Unified Manager gera um alerta somente quando um evento atende aos critérios de filtro especificados. Você pode escolher os eventos para os quais os alertas devem ser gerados - por exemplo, quando um limite de espaço é excedido ou um objeto fica offline. Você também pode associar um alerta a um script que é executado quando um alerta é acionado.

Os critérios de filtro incluem classe de objeto, nome ou gravidade do evento.

### 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 ou limite violado 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.

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 Active IQ 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 Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento é gerado.
- Você deve saber os recursos e eventos para os quais deseja acionar o alerta e os nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se você quiser que um script seja executado com base no evento, você deve ter adicionado o script ao Unified Manager usando a página Scripts.
- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

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

### Passos

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

2. Na página **Configuração de alerta**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar alerta**, clique em **Nome** e insira um nome e uma descrição para o alerta.
4. Clique em **recursos** e selecione os recursos a serem incluídos ou excluídos do alerta.

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

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

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



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

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



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

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

7. Clique em **Salvar**.

### Exemplo de adição de um alerta

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

- Nome do alerta: HealthTest
- Recursos: Inclui todos os volumes cujo nome contém "abc" e exclui todos os volumes cujo nome contém "xyz"
- Eventos: Inclui todos os eventos críticos de saúde
- Ações: Inclui "[sample@domain.com](mailto:sample@domain.com)", um script "Test", e o usuário deve ser notificado a cada 15 minutos

Execute as seguintes etapas na caixa de diálogo Adicionar alerta:

1. Clique em **Nome** e digite **HealthTest** no campo **Nome do alerta**.
2. Clique em **recursos** e, na guia incluir, selecione **volumes** na lista suspensa.
  - a. **abc`Digite \* no campo \*Nome contém** para exibir os volumes cujo nome contém "abc".
  - b. Selecione **\*[All Volumes whose name contains 'abc']** na área recursos disponíveis e mova-o para a área recursos selecionados.

- c. Clique em **Excluir** e digite **xyz** no 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 digite **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**.

### Diretrizes para adicionar alertas

Você pode adicionar alertas com base em um recurso, como um cluster, nó, agregado ou volume, e eventos de um tipo de gravidade específico. Como prática recomendada, você pode adicionar um alerta para qualquer um dos seus objetos críticos depois de adicionar o cluster ao qual o objeto pertence.

Você pode usar as seguintes diretrizes e considerações para criar alertas para gerenciar seus sistemas de forma eficaz:

- Descrição do alerta

Você deve fornecer uma descrição para o alerta para que ele o ajude a rastrear seus alertas de forma eficaz.

- Recursos

Você deve decidir qual recurso físico ou lógico requer um alerta. Você pode incluir e excluir recursos, conforme necessário. Por exemplo, se você quiser monitorar de perto seus agregados configurando um alerta, selecione os agregados necessários na lista de recursos.

Se você selecionar uma categoria de recursos, por exemplo, [\[All User or Group Quotas\]](#) você receberá alertas para todos os objetos nessa categoria.



A seleção de um cluster como recurso não seleciona automaticamente os objetos de armazenamento dentro desse cluster. Por exemplo, se você criar um alerta para todos os eventos críticos para todos os clusters, receberá alertas apenas para eventos críticos do cluster. Você não receberá alertas de eventos críticos em nós, agregados e assim por diante.

- Gravidade do evento

Você deve decidir se um evento de um tipo de gravidade especificado (crítico, erro, aviso) deve acionar o alerta e, em caso afirmativo, qual tipo de gravidade.

- Eventos selecionados

Se você adicionar um alerta com base no tipo de evento gerado, você deve decidir quais eventos exigem



um alerta.

Se você selecionar uma gravidade de evento, mas não selecionar nenhum evento individual (se você deixar a coluna "Eventos selecionados" vazia), receberá alertas para todos os eventos da categoria.

- **Ações**

Você deve fornecer os nomes de usuário e endereços de e-mail dos usuários que recebem a notificação. Você também pode especificar uma trap SNMP como um modo de notificação. Você pode associar seus scripts a um alerta para que eles sejam executados quando um alerta é gerado.

- **Frequência da notificação**

Você pode configurar um alerta para enviar notificações repetidamente aos destinatários por um tempo especificado. Você deve determinar a hora a partir da qual a notificação de evento está ativa para o alerta. Se você quiser que a notificação de evento seja repetida até que o evento seja reconhecido, você deve determinar com que frequência deseja que a notificação seja repetida.

- **Execute Script**

Você pode associar seu script a um alerta. Seu script é executado quando o alerta é gerado.

## 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

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

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 **Gerenciamento de armazenamento > Configuração de alerta**.
2. Na página **Configuração de alerta**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar alerta**, clique em **Nome** e insira um nome e uma descrição para o alerta.
4. 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 traps SNMP e executar um script.
8. Clique em **Salvar**.

## Testando alertas

Pode testar um alerta para verificar se o configurou corretamente. Quando um evento é acionado, um alerta é gerado e um e-mail de alerta é enviado aos destinatários configurados. Você pode verificar se a notificação é enviada e se o script é executado usando o alerta de teste.

### Antes de começar

- Você deve ter configurado configurações de notificação, como o endereço de e-mail dos destinatários, servidor SMTP e trap SNMP.

O servidor do Unified Manager pode usar essas configurações para enviar notificações aos usuários quando um evento é gerado.

- Você deve ter atribuído um script e configurado o script para ser executado quando o alerta é gerado.
- Tem de ter a função Administrador de aplicações.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de alerta**.
2. Na página **Configuração de alerta**, selecione o alerta que deseja testar e clique em **Teste**.

Um e-mail de alerta de teste é enviado para os endereços de e-mail especificados durante a criação do alerta.

## Ativar e desativar alertas para eventos resolvidos e obsoletos

Para todos os eventos que você configurou para enviar alertas, uma mensagem de alerta é enviada quando esses eventos passam por todos os estados disponíveis: Novo, confirmado, resolvido e Obsoleto. Se você não quiser receber alertas de eventos à medida que eles se movem para os estados resolvidos e obsoletos, você pode configurar uma configuração global para suprimir esses alertas.

### Antes de começar

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

Por padrão, os alertas não são enviados para eventos à medida que se movem para os estados resolvido e Obsoleto.

## Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de alerta**.
2. Na página **Configuração de alerta**, execute uma das seguintes ações usando o controle deslizante ao lado do item **Alertas para eventos resolvidos e obsoletos**:

Para...	Faça isso...
Pare de enviar alertas à medida que os eventos são resolvidos ou obsoletos	Mova o controle deslizante para a esquerda
Comece a enviar alertas à medida que os eventos forem resolvidos ou obsoletos	Mova o controle deslizante para a direita

## Exclusão da geração de alertas de volumes de destino de recuperação de desastres

Ao configurar alertas de volume, você pode especificar uma cadeia de caracteres na caixa de diálogo Alerta que identifica um volume ou grupo de volumes. No entanto, se você configurou a recuperação de desastres para SVMs, os volumes de origem e destino têm o mesmo nome, então você receberá alertas para ambos os volumes.

### Antes de começar

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

Você pode desativar alertas de volumes de destino de recuperação de desastres excluindo volumes que tenham o nome do SVM de destino. Isso é possível porque o identificador para eventos de volume contém o nome do SVM e o nome do volume no formato "<svm\_name>:/<volume\_name>".

O exemplo abaixo mostra como criar alertas para o volume "vol1" no SVM principal "VS1", mas exclui que o alerta seja gerado em um volume com o mesmo nome no SVM "VS1-dr".

Execute as seguintes etapas na caixa de diálogo Adicionar alerta:

### Passos

1. Clique em **Nome** e insira um nome e uma descrição para o alerta.
2. Clique em **recursos** e selecione a guia **incluir**.
  - a. Selecione **volume** na lista suspensa e digite **vol1** no campo **Nome contém** para exibir os volumes cujo nome contém "vol1".
  - b. Selecione **[All Volumes whose name contains 'vol1']** na área **\*recursos disponíveis** e mova-a para a área **recursos selecionados**.
3. Selecione a guia **Excluir**, selecione **volume**, digite **vs1-dr** no campo **Nome contém** e clique em **Adicionar**.

Isso exclui que o alerta seja gerado para o volume "vol1" na SVM "VS1-dr".

4. Clique em **Eventos** e selecione o evento ou eventos que deseja aplicar ao volume ou volumes.
5. Clique em **ações** e selecione o nome do usuário que receberá o e-mail de alerta no campo **alertar esses**

## usuários.

6. Configure quaisquer outras opções nesta página para emitir traps SNMP e executar um script e, em seguida, clique em **Salvar**.

## Visualização de alertas

Pode ver a lista de alertas criados para vários eventos a partir da página Configuração de alertas. Você também pode exibir propriedades de alerta, como a descrição do alerta, o método e a frequência da notificação, os eventos que acionam o alerta, os destinatários de e-mail dos alertas e os recursos afetados, como clusters, agregados e volumes.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

### Passo

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

A lista de alertas é exibida na página Configuração de alertas.

## Editar alertas

Você pode editar propriedades de alerta, como o recurso com o qual o alerta está associado, eventos, destinatários, opções de notificação, frequência de notificação e scripts associados.

### Antes de começar

Tem de ter a função Administrador de aplicações.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de alerta**.
2. Na página **Configuração de alerta**, selecione o alerta que deseja editar e clique em **Editar**.
3. Na caixa de diálogo **Editar alerta**, edite as seções nome, recursos, eventos e ações, conforme necessário.

Você pode alterar ou remover o script associado ao alerta.

4. Clique em **Salvar**.

## Eliminar alertas

Você pode excluir um alerta quando ele não for mais necessário. Por exemplo, você pode excluir um alerta criado para um recurso específico quando esse recurso não for mais monitorado pelo Unified Manager.

### Antes de começar

Tem de ter a função Administrador de aplicações.

## Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de alerta**.
2. Na página **Configuração de alerta**, selecione os alertas que deseja excluir e clique em **Excluir**.
3. Clique em **Yes** para confirmar a solicitação de exclusão.

## Descrição das janelas de alerta e caixas de diálogo

Você deve configurar alertas para receber notificações sobre eventos usando a caixa de diálogo Adicionar alerta. Também pode ver a lista de alertas na página Configuração de alertas.

### Página Configuração de alerta

A página Configuração de alertas exibe uma lista de alertas e fornece informações sobre o nome, o status, o método de notificação e a frequência de notificação do alerta. Você também pode adicionar, editar, remover, ativar ou desativar alertas desta página.

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

### Botões de comando

- **Adicionar**

Exibe a caixa de diálogo Adicionar alerta, que permite adicionar novos alertas.

- **Editar**

Exibe a caixa de diálogo Editar alerta, que permite editar alertas selecionados.

- **Excluir**

Elimina os alertas selecionados.

- **Ativar**

Ativa os alertas selecionados para enviar notificações.

- **Desativar**

Desativa os alertas selecionados quando você deseja interromper temporariamente o envio de notificações.

- **Teste**

Testa os alertas selecionados para verificar sua configuração depois de serem adicionados ou editados.

- **Alertas para Eventos resolvidos e obsoletos**

Permite-lhe ativar ou desativar o envio de alertas quando os eventos são movidos para os estados resolvidos ou obsoletos. Isso pode ajudar os usuários a não receber notificações desnecessárias.

## Vista de lista

A exibição de lista exibe, em formato tabular, informações sobre os alertas criados. Você pode usar os filtros de coluna para personalizar os dados exibidos. Você também pode selecionar um alerta para exibir mais informações sobre ele na área de detalhes.

- **Status**

Especifica se um alerta está ativado () ou desativado (.

- **Alerta**

Exibe o nome do alerta.

- **Descrição**

Exibe uma descrição para o alerta.

- **Método de notificação**

Exibe o método de notificação selecionado para o alerta. Você pode notificar os usuários através de traps de e-mail ou SNMP.

- **Frequência de notificação**

Especifica a frequência (em minutos) com a qual o servidor de gerenciamento continua a enviar notificações até que o evento seja reconhecido, resolvido ou movido para o estado Obsoleto.

## Área de detalhes

A área de detalhes fornece mais informações sobre o alerta selecionado.

- **Nome do alerta**

Exibe o nome do alerta.

- **Descrição do alerta**

Exibe uma descrição para o alerta.

- **Eventos**

Exibe os eventos para os quais você deseja acionar o alerta.

- **Recursos**

Exibe os recursos para os quais você deseja acionar o alerta.

- **Inclui**

Exibe o grupo de recursos para os quais você deseja acionar o alerta.

- **Exclui**

Exibe o grupo de recursos para os quais você não deseja acionar o alerta.

- **Método de notificação**

Exibe o método de notificação para o alerta.

- **Frequência de notificação**

Exibe a frequência com que o servidor de gerenciamento continua a enviar notificações de alerta até que o evento seja reconhecido, resolvido ou movido para o estado Obsoleto.

- **Nome do Script**

Exibe o nome do script associado ao alerta selecionado. Este script é executado quando um alerta é gerado.

- **Destinatários de e-mail**

Exibe os endereços de e-mail dos usuários que recebem a notificação de alerta.

### Caixa de diálogo Adicionar alerta

Você pode criar alertas para notificá-lo quando um evento específico é gerado, para que você possa resolver o problema rapidamente e, assim, minimizar o impactos no seu ambiente. Você pode criar alertas para um único recurso ou um conjunto de recursos e para eventos de um tipo de gravidade específico. Você também pode especificar o método de notificação e a frequência dos alertas.

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

#### Nome

Esta área permite especificar um nome e uma descrição para o alerta:

- **Nome do alerta**

Permite especificar um nome de alerta.

- **Descrição do alerta**

Permite especificar uma descrição para o alerta.

#### Recursos

Essa área permite selecionar um recurso individual ou agrupar os recursos com base em uma regra dinâmica para a qual você deseja acionar o alerta. Uma regra *dinâmica* é o conjunto de recursos filtrados com base na cadeia de texto especificada. Você pode pesquisar recursos selecionando um tipo de recurso na lista suspensão ou especificar o nome exato do recurso para exibir um recurso específico.

Se você estiver criando um alerta a partir de qualquer uma das páginas de detalhes do objeto de armazenamento, o objeto de armazenamento será incluído automaticamente no alerta.

- **Incluir**

Permite incluir os recursos para os quais você deseja acionar alertas. Você pode especificar uma cadeia

de texto para agrupar recursos que correspondem à cadeia de caracteres e selecionar esse grupo a ser incluído no alerta. Por exemplo, você pode agrupar todos os volumes cujo nome contém a string "abc".

- **Excluir**

Permite excluir recursos para os quais você não deseja acionar alertas. Por exemplo, você pode excluir todos os volumes cujo nome contém a string "xyz".

A guia Excluir é exibida somente quando você seleciona todos os recursos de um tipo de recurso específico: Por exemplo, [\[All Volumes\]](#) [\[All Volumes whose name contains 'xyz'\]](#)

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 o evento.

## Eventos

Esta área permite-lhe selecionar os eventos para os quais pretende criar os alertas. Você pode criar alertas para eventos com base em uma gravidade específica ou em um conjunto de eventos.

Para selecionar mais de um evento, mantenha pressionada a tecla Ctrl enquanto faz as seleções.

- **Gravidade do evento**

Permite selecionar eventos com base no tipo de gravidade, que pode ser crítico, erro ou Aviso.

- **Nome do evento contém**

Permite selecionar eventos cujo nome contém caracteres especificados.

## Ações

Essa área permite especificar os usuários que você deseja notificar quando um alerta é acionado. Você também pode especificar o método de notificação e a frequência da notificação.

- **Alertar esses usuários**

Permite especificar o endereço de e-mail ou o nome de usuário do usuário para receber notificações.

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 tiver modificado o endereço de e-mail do usuário selecionado na página usuários, o endereço de e-mail modificado não será atualizado para o usuário selecionado.

- **Frequência de notificação**

Permite especificar a frequência com que o servidor de gerenciamento envia notificações até que o evento seja reconhecido, resolvido ou movido para o estado obsoleto.

Você pode escolher os seguintes métodos de notificação:

- Notificar apenas uma vez
- Notificar a uma frequência especificada
- Notificar a uma frequência especificada dentro do intervalo de tempo especificado



- **Emitir trap SNMP**

Selecionar esta caixa permite especificar se as traps SNMP devem ser enviadas para o host SNMP configurado globalmente.

- **Execute Script**

Permite-lhe adicionar o seu script personalizado ao alerta. Este script é executado quando um alerta é gerado.



Se você não vir esse recurso disponível na interface do usuário, é porque a funcionalidade foi desativada pelo administrador. Se necessário, pode ativar esta funcionalidade a partir de **Gestão de armazenamento > Definições de funcionalidade**.

#### Botões de comando

- **Guardar**

Cria um alerta e fecha a caixa de diálogo.

- **Cancelar**

Descarta as alterações e fecha a caixa de diálogo.

#### Caixa de diálogo Editar alerta

Você pode editar propriedades de alerta, como o recurso com o qual o alerta está associado, eventos, script e opções de notificação.

#### Nome

Esta área permite editar o nome e a descrição do alerta.

- **Nome do alerta**

Permite editar o nome do alerta.

- **Descrição do alerta**

Permite especificar uma descrição para o alerta.

- **Estado de alerta**

Permite ativar ou desativar o alerta.

#### Recursos

Essa área permite selecionar um recurso individual ou agrupar os recursos com base em uma regra dinâmica para a qual você deseja acionar o alerta. Você pode pesquisar recursos selecionando um tipo de recurso na lista suspensa ou especificar o nome exato do recurso para exibir um recurso específico.

- **Incluir**

Permite incluir os recursos para os quais você deseja acionar alertas. Você pode especificar uma cadeia de texto para agrupar recursos que correspondem à cadeia de caracteres e selecionar esse grupo a ser incluído no alerta. Por exemplo, você pode agrupar todos os volumes cujo nome contém a string "vol0".

- **Excluir**

Permite excluir recursos para os quais você não deseja acionar alertas. Por exemplo, você pode excluir todos os volumes cujo nome contém a string "xyz".



A guia Excluir é exibida somente quando você seleciona todos os recursos de um tipo de recurso específico. [\[All Volumes\]](#) [\[All Volumes whose name contains 'xyz'\]](#)

## Eventos

Esta área permite-lhe selecionar os eventos para os quais pretende acionar os alertas. Você pode acionar um alerta para eventos com base em uma gravidade específica ou em um conjunto de eventos.

- **Gravidade do evento**

Permite selecionar eventos com base no tipo de gravidade, que pode ser crítico, erro ou Aviso.

- **Nome do evento contém**

Permite selecionar eventos cujo nome contém os caracteres especificados.

## Ações

Esta área permite especificar o método de notificação e a frequência da notificação.

- **Alertar esses usuários**

Permite editar o endereço de e-mail ou o nome de usuário ou especificar um novo endereço de e-mail ou nome de usuário para receber notificações.

- **Frequência de notificação**

Permite editar a frequência com que o servidor de gerenciamento envia notificações até que o evento seja reconhecido, resolvido ou movido para o estado obsoleto.

Você pode escolher os seguintes métodos de notificação:

- Notificar apenas uma vez
- Notificar a uma frequência especificada
- Notificar a uma frequência especificada dentro do intervalo de tempo especificado

- **Emitir trap SNMP**

Permite especificar se as traps SNMP devem ser enviadas para o host SNMP configurado globalmente.

- **Execute Script**

Permite associar um script ao alerta. Este script é executado quando um alerta é gerado.

## Botões de comando

- **Guardar**

Salva as alterações e fecha a caixa de diálogo.

- **Cancelar**

Descarta as alterações e fecha a caixa de diálogo.

## Gerenciamento de scripts

Você pode usar scripts para modificar ou atualizar automaticamente vários objetos de armazenamento no Unified Manager. O script está associado a um alerta. Quando um evento aciona um alerta, o script é executado. Você pode carregar scripts personalizados e testar sua execução quando um alerta é gerado.

A capacidade de carregar scripts para o Unified Manager e executá-los é ativada por padrão. Se a sua organização não quiser permitir esta funcionalidade por motivos de segurança, pode desativar esta funcionalidade a partir de **Gestão de armazenamento > Definições de funcionalidade**.

### Informações relacionadas

["Ativar e desativar a capacidade de carregar scripts"](#)

### Como os scripts funcionam com alertas

Você pode associar um alerta ao script para que o script seja executado quando um alerta for gerado para um evento no Unified Manager. Você pode usar os scripts para resolver problemas com objetos de armazenamento ou identificar quais objetos de armazenamento estão gerando os eventos.

Quando um alerta é gerado para um evento no Unified Manager, um e-mail de alerta é enviado aos destinatários especificados. Se você associou um alerta a um script, o script será executado. Você pode obter os detalhes dos argumentos passados para o script a partir do e-mail de alerta.



Se você criou um script personalizado e o associou a um alerta para um tipo de evento específico, as ações serão realizadas com base no script personalizado para esse tipo de evento e as ações **Fix it** não estarão disponíveis por padrão na página ações de gerenciamento ou no painel do Unified Manager.

O script usa os seguintes argumentos para execução:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`

- -eventSourceType
- -eventState
- -eventArgs

Você pode usar os argumentos em seus scripts e coletar informações de eventos relacionados ou modificar objetos de armazenamento.

### Exemplo para obter argumentos de scripts

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

Quando um alerta é gerado, este script é executado e a seguinte saída é exibida:

```
-`eventID : 290`
-`eventSourceID : 4138`
```

### Adicionando scripts

Você pode adicionar scripts no Unified Manager e associar os scripts a alertas. Esses scripts são executados automaticamente quando um alerta é gerado e permitem obter informações sobre objetos de armazenamento para os quais o evento é gerado.

#### Antes de começar

- Você deve ter criado e salvo os scripts que deseja adicionar ao servidor do Unified Manager.
- Os formatos de arquivo suportados para scripts são Perl, Shell, PowerShell, Python e .bat arquivos.

Plataforma na qual o Unified Manager está instalado	Idiomas suportados
VMware	Scripts Perl e Shell
Linux	Scripts Perl, Python e Shell
Windows	Scripts PowerShell, Perl, Python e .bat

- Para scripts Perl, Perl deve ser instalado no servidor Unified Manager. Para instalações VMware, o Perl 5 é instalado por padrão e os scripts suportam apenas o que o Perl 5 suporta. Se o Perl foi instalado após o Unified Manager, você deve reiniciar o servidor do Unified Manager.
- Para scripts do PowerShell, a política de execução apropriada do PowerShell deve ser definida no servidor Windows para que os scripts possam ser executados.



Se o script criar arquivos de log para acompanhar o andamento do script de alerta, você deve garantir que os arquivos de log não sejam criados em qualquer lugar na pasta de instalação do Unified Manager.

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

Você pode fazer upload de scripts personalizados e reunir detalhes do evento sobre o alerta.



Se você não vir esse recurso disponível na interface do usuário, é porque a funcionalidade foi desativada pelo administrador. Se necessário, pode ativar esta funcionalidade a partir de **Gestão de armazenamento > Definições de funcionalidade**.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Scripts**.
2. Na página **Scripts**, clique em **Add**.
3. Na caixa de diálogo **Add Script**, clique em **Browse** para selecionar seu arquivo de script.
4. Insira uma descrição para o script selecionado.
5. Clique em **Add**.

### Informações relacionadas

["Ativar e desativar a capacidade de carregar scripts"](#)

## Eliminar scripts

Você pode excluir um script do Unified Manager quando o script não for mais necessário ou válido.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- O script não deve estar associado a um alerta.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Scripts**.
2. Na página **Scripts**, selecione o script que deseja excluir e clique em **Delete**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

## Testando a execução de script

Você pode verificar se o script é executado corretamente quando um alerta é gerado para um objeto de armazenamento.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter carregado um script no formato de arquivo suportado para o Unified Manager.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Scripts**.
2. Na página **Scripts**, adicione seu script de teste.
3. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de alerta**.

4. Na página **Configuração de alerta**, execute uma das seguintes ações:

Para...	Faça isso...
Adicione um alerta	a. Clique em <b>Add</b> . b. Na seção ações, associe o alerta ao script de teste.
Edite um alerta	a. Selecione um alerta e clique em <b>Editar</b> . b. Na seção ações, associe o alerta ao script de teste.

5. Clique em **Salvar**.

6. Na página **Configuração de alerta**, selecione o alerta que você adicionou ou modificou e clique em **Teste**.

O script é executado com o argumento "-teste", e um alerta de notificação é enviado para os endereços de e-mail que foram especificados quando o alerta foi criado.

## Comandos de CLI do Unified Manager compatíveis

Como administrador de storage, você pode usar os comandos de CLI para executar consultas nos objetos de storage, por exemplo, em clusters, agregados, volumes, qtrees e LUNs. Você pode usar os comandos CLI para consultar o banco de dados interno do Unified Manager e o banco de dados do ONTAP. Você também pode usar comandos CLI em scripts que são executados no início ou no final de uma operação ou que são executados quando um alerta é acionado.

Todos os comandos devem ser precedidos com o comando `um cli login` e um nome de usuário e senha válidos para autenticação.



Para executar o comando `um RUN`, certifique-se de que sua conta tenha acesso ao aplicativo *console*.

Comando CLI	Descrição	Saída
<pre>um cli login -u &lt;username&gt; [-p &lt;password&gt;]</pre>	<p>Inicia sessão na CLI. Devido a implicações de segurança, você deve inserir apenas o nome de usuário seguindo a opção "-u". Quando usada desta maneira, você será solicitado a fornecer a senha e a senha não será capturada na tabela de histórico ou processo. A sessão expira após três horas a partir do momento do login, após o qual o usuário deve fazer login novamente.</p>	<p>Exibe a mensagem correspondente.</p>

<b>Comando CLI</b>	<b>Descrição</b>	<b>Saída</b>
<code>um cli logout</code>	Faz logout da CLI.	Exibe a mensagem correspondente.
<code>um help</code>	Exibe todos os subcomandos de primeiro nível.	Exibe todos os subcomandos de primeiro nível.
<code>um run cmd [ -t &lt;timeout&gt; ] &lt;cluster&gt; &lt;command&gt;</code>	A maneira mais simples de executar um comando em um ou mais hosts. Usado principalmente para scripts de alerta para obter ou executar uma operação no ONTAP. O argumento opcional timeout define um limite máximo de tempo (em segundos) para que o comando seja concluído no cliente. O padrão é 0 (espere para sempre).	Como recebido de ONTAP.
<code>um run query &lt;sql command&gt;</code>	Executa uma consulta SQL. Somente consultas que leem a partir do banco de dados são permitidas. Qualquer operação de atualização, inserção ou exclusão não é suportada.	Os resultados são exibidos em uma forma tabular. Se um conjunto vazio for retornado, ou se houver algum erro de sintaxe ou solicitação incorreta, ele exibirá a mensagem de erro apropriada.
<code>um datasource add -u &lt;username&gt; -P &lt;password&gt; [ -t &lt;protocol&gt; ] [ -p &lt;port&gt; ] &lt;hostname-or-ip&gt;</code>	Adiciona uma fonte de dados à lista de sistemas de armazenamento gerenciados. Uma fonte de dados descreve como as conexões com sistemas de armazenamento são feitas. As opções -u (nome de usuário) e -P (senha) devem ser especificadas ao adicionar uma fonte de dados. A opção -t (protocolo) especifica o protocolo usado para se comunicar com o cluster (http ou https). Se o protocolo não for especificado, ambos os protocolos serão tentados a opção -p (porta) especifica a porta usada para se comunicar com o cluster. Se a porta não for especificada, então o valor padrão do protocolo apropriado será tentado. Este comando só pode ser executado pelo administrador de armazenamento.	Solicita que o usuário aceite o certificado e imprime a mensagem correspondente.

Comando CLI	Descrição	Saída
um datasource list [ <datasource-id> ]	Exibe as fontes de dados para sistemas de armazenamento gerenciados.	Exibe os seguintes valores em formato tabular: ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.
um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>	Modifica uma ou mais opções de fonte de dados. Só pode ser executado pelo administrador de armazenamento.	Exibe a mensagem correspondente.
um datasource remove <datasource-id>	Remove a fonte de dados (cluster) do Unified Manager.	Exibe a mensagem correspondente.
um option list [ <option> .. ]	Lista todas as opções que você pode configurar usando o comando SET.	Exibe os seguintes valores em formato tabular: Name, Value, Default Value, and Requires Restart.
um option set <option-name>=<option-value> [ <option-name>=<option-value> ... ]	Define uma ou mais opções. O comando só pode ser executado pelo administrador de armazenamento.	Exibe a mensagem correspondente.
um version	Exibe a versão do software Unified Manager.	Version ("9.6")
um lun list [-q] [ -ObjectType <object-id> ]	<p>Lista os LUNs após a filtragem no objeto especificado. -q é aplicável para todos os comandos para mostrar nenhum cabeçalho. ObjectType pode ser lun, qtree, cluster, volume, cota ou svm.</p> <p>Por exemplo:</p> <p><b>um lun list -cluster 1</b></p> <p>Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os LUNs dentro do cluster com ID 1.</p>	Exibe os seguintes valores em formato tabular: ID and LUN path.



Comando CLI	Descrição	Saída
<pre>um svm list [-q] [-ObjectType &lt;object-id&gt;]</pre>	<p>Lista as VMs de armazenamento após a filtragem no objeto especificado. ObjectType pode ser lun, qtree, cluster, volume, cota ou svm.</p> <p>Por exemplo:</p> <p><b>um svm list -cluster 1</b></p> <p>Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todas as VMs de armazenamento dentro do cluster com ID 1.</p>	<p>Exibe os seguintes valores em formato tabular: Name and Cluster ID.</p>
<pre>um qtree list [-q] [-ObjectType &lt;object-id&gt;]</pre>	<p>Lista os qtrees após a filtragem no objeto especificado. -q é aplicável para todos os comandos para mostrar nenhum cabeçalho. ObjectType pode ser lun, qtree, cluster, volume, cota ou svm.</p> <p>Por exemplo:</p> <p><b>um qtree list -cluster 1</b></p> <p>Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os qtrees dentro do cluster com ID 1.</p>	<p>Exibe os seguintes valores em formato tabular: Qtree ID and Qtree Name.</p>
<pre>um disk list [-q] [-ObjectType &lt;object-id&gt;]</pre>	<p>Lista os discos após a filtragem no objeto especificado. ObjectType pode ser disco, aggr, nó ou cluster.</p> <p>Por exemplo:</p> <p><b>um disk list -cluster 1</b></p> <p>Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os discos dentro do cluster com ID 1.</p>	<p>Exibe os seguintes valores em formato tabular ObjectType and object-id.</p>

Comando CLI	Descrição	Saída
<pre>um cluster list [-q] [-Objectype &lt;object-id&gt;]</pre>	<p>Lista os clusters após a filtragem no objeto especificado. Objectype pode ser disco, aggr, nó, cluster, lun, qtree, volume, cota ou svm.</p> <p>Por exemplo:</p> <p><b>um cluster list -aggr 1</b></p> <p>Neste exemplo, "-aggr" é o objectype e "1" é o objectId. O comando lista o cluster ao qual o agregado com ID 1 pertence.</p>	<p>Exibe os seguintes valores em formato tabular: Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.</p>
<pre>um cluster node list [-q] [-Objectype &lt;object-id&gt;]</pre>	<p>Lista os nós de cluster após a filtragem no objeto especificado. Objectype pode ser disco, aggr, nó ou cluster.</p> <p>Por exemplo:</p> <p><b>um cluster node list -cluster 1</b></p> <p>Neste exemplo, "-cluster" é o objectype e "1" é o objectId. O comando lista todos os nós dentro do cluster com ID 1.</p>	<p>Exibe os seguintes valores em formato tabular Name and Cluster ID.</p>
<pre>um volume list [-q] [-Objectype &lt;object-id&gt;]</pre>	<p>Lista os volumes após a filtragem no objeto especificado. Objectype pode ser lun, qtree, cluster, volume, cota, svm ou agregado.</p> <p>Por exemplo:</p> <p><b>um volume list -cluster 1</b></p> <p>Neste exemplo, "-cluster" é o objectype e "1" é o objectId. O comando lista todos os volumes dentro do cluster com ID 1.</p>	<p>Exibe os seguintes valores em formato tabular Volume ID and Volume Name .</p>

Comando CLI	Descrição	Saída
um quota user list [-q] [-ObjectType <object-id>]	<p>Lista os usuários de cota após a filtragem no objeto especificado. ObjectType pode ser qtree, cluster, volume, cota ou svm.</p> <p>Por exemplo:</p> <pre><b>um quota user list -cluster 1</b></pre> <p>Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os usuários de cota dentro do cluster com ID 1.</p>	Exibe os seguintes valores em formato tabular ID, Name, SID and Email .
um aggr list [-q] [-ObjectType <object-id>]	<p>Lista os agregados após a filtragem no objeto especificado. ObjectType pode ser disco, aggr, nó, cluster ou volume.</p> <p>Por exemplo:</p> <pre><b>um aggr list -cluster 1</b></pre> <p>Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os agregados dentro do cluster com ID 1.</p>	Exibe os seguintes valores em formato tabular Aggr ID, and Aggr Name .
um event ack <event-ids>	Reconhece um ou mais eventos.	Exibe a mensagem correspondente.
um event resolve <event-ids>	Resolve um ou mais eventos.	Exibe a mensagem correspondente.
um event assign -u <username> <event-id>	Atribui um evento a um usuário.	Exibe a mensagem correspondente.
um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]	Lista os eventos gerados pelo sistema ou usuário. Filtra eventos com base na origem, estado e IDs.	Exibe os seguintes valores em formato tabular Source, Source type, Name, Severity, State, User and Timestamp .
um backup restore -f <backup_file_path_and_name>	Restaura um backup de banco de dados MySQL usando arquivos .7z.	Exibe a mensagem correspondente.

## Descrição das janelas de script e caixas de diálogo

A página Scripts permite adicionar scripts ao Unified Manager.

### Página de scripts

A página Scripts permite adicionar seus scripts personalizados ao Unified Manager. Você pode associar esses scripts a alertas para habilitar a reconfiguração automática de objetos de storage.

A página Scripts permite adicionar ou excluir scripts do Unified Manager.

### Botões de comando

- **Adicionar**

Exibe a caixa de diálogo Adicionar script, que permite adicionar scripts.

- **Excluir**

Exclui o script selecionado.

### Vista de lista

A exibição de lista exibe, em formato tabular, os scripts adicionados ao Unified Manager.

- **Nome**

Exibe o nome do script.

- **Descrição**

Exibe a descrição do script.

### Caixa de diálogo Add Script (Adicionar script)

A caixa de diálogo Adicionar script permite adicionar scripts ao Unified Manager. Você pode configurar alertas com seus scripts para resolver automaticamente eventos gerados para objetos de armazenamento.

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

- **Selecione Arquivo de Script**

Permite selecionar um script para o alerta.

- **Descrição**

Permite especificar uma descrição para o script.

# Monitorar e gerenciar o desempenho do cluster

## Introdução ao monitoramento de desempenho do Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente chamado Gerenciador Unificado de OnCommand) fornece recursos de monitoramento de desempenho e análise de causa-raiz de eventos para sistemas que executam o software NetApp ONTAP.

O Unified Manager ajuda você a identificar workloads que estão sobrecarregando componentes do cluster e diminuindo o desempenho de outros workloads no cluster. Ao definir políticas de limite de desempenho, você também pode especificar valores máximos para determinados contadores de desempenho para que os eventos sejam gerados quando o limite for violado. O Unified Manager alerta você sobre esses eventos de performance para que você tome medidas corretivas e coloque a performance de volta ao nível normal de operação. Você pode exibir e analisar eventos na IU do Unified Manager.

O Unified Manager monitora a performance de dois tipos de workloads:

- Workloads definidos pelo usuário

Esses workloads consistem em FlexVol volumes e FlexGroup volumes criados no cluster.

- Workloads definidos pelo sistema

Esses workloads consistem em atividade interna do sistema.

## Recursos de monitoramento de desempenho do Unified Manager

O Unified Manager coleta e analisa estatísticas de performance de sistemas que executam o software ONTAP. Ele usa limites de desempenho dinâmicos e limites de desempenho definidos pelo usuário para monitorar uma variedade de contadores de desempenho em vários componentes do cluster.

Um alto tempo de resposta (latência) indica que o objeto de armazenamento, por exemplo, um volume, está funcionando mais lento do que o normal. Esse problema também indica que o desempenho diminuiu para aplicativos clientes que estão usando o volume. O Unified Manager identifica o componente de storage em que reside o problema de performance e fornece uma lista das ações sugeridas que você pode tomar para solucionar o problema de performance.

O Unified Manager inclui os seguintes recursos:

- Monitora e analisa as estatísticas de performance de workload a partir de um sistema que executa o software ONTAP.
- Controla os contadores de performance de clusters, nós, agregados, portas, SVMs, volumes, LUNs, namespaces NVMe e interfaces de rede (LIFs).
- Exibe gráficos detalhados que plotam a atividade da carga de trabalho ao longo do tempo, incluindo IOPS (operações), MB/s (taxa de transferência), latência (tempo de resposta), utilização, capacidade de performance e taxa de cache.
- Permite criar políticas de limite de performance definidas pelo usuário que acionam eventos e enviam

alertas de e-mail quando os limites são violados.

- Usa limites definidos pelo sistema e limites de performance dinâmicos que aprendem sobre sua atividade de workload para identificar e alertar você sobre problemas de performance.
- Identifica as políticas de qualidade do serviço (QoS) e as políticas de nível de serviço (PSLs) de performance aplicadas aos volumes e LUNs.
- Identifica claramente o componente do cluster que está em disputa.
- Identifica cargas de trabalho que estão sobreusando componentes do cluster e as cargas de trabalho cujo desempenho é afetado pelo aumento da atividade.

## Interfaces do Unified Manager usadas para gerenciar a performance do sistema de storage

Essas seções contêm informações sobre as duas interfaces de usuário fornecidas pelo Active IQ Unified Manager para solucionar problemas de capacidade, disponibilidade e proteção de storage de dados. As duas UIs são a IU da Web do Unified Manager e o console de manutenção.

Se você quiser usar os recursos de proteção no Unified Manager, também deverá instalar e configurar o OnCommand Workflow Automation (WFA).

### IU da Web do Unified Manager

A IU da Web do Unified Manager permite que um administrador monitore e solucione problemas de cluster relacionados à capacidade, disponibilidade e proteção de storage de dados.

Essas seções descrevem alguns fluxos de trabalho comuns que um administrador pode seguir para solucionar problemas de capacidade de storage, disponibilidade de dados ou proteção exibidos na IU da Web do Unified Manager.

### Consola de manutenção

O console de manutenção do Unified Manager permite que um administrador monitore, diagnostique e solucione problemas do sistema operacional, problemas de atualização de versão, problemas de acesso do usuário e problemas de rede relacionados ao próprio servidor do Unified Manager. Se a IU da Web do Unified Manager não estiver disponível, o console de manutenção será a única forma de acesso ao Unified Manager.

Você pode usar essas informações para acessar o console de manutenção e usá-lo para resolver problemas relacionados ao funcionamento do servidor do Unified Manager.

## Atividade de coleta de dados de desempenho e configuração de cluster

O intervalo de coleta para *cluster Configuration data* é de 15 minutos. Por exemplo, depois de adicionar um cluster, leva 15 minutos para exibir os detalhes do cluster na IU do Unified Manager. Este intervalo também se aplica ao fazer alterações em um cluster.

Por exemplo, se você adicionar dois novos volumes a um SVM em um cluster, verá esses novos objetos na IU após o próximo intervalo de polling, que pode ser de até 15 minutos.

O Unified Manager coleta *estatísticas de desempenho* atuais de todos os clusters monitorados a cada cinco minutos. Ele analisa esses dados para identificar eventos de desempenho e possíveis problemas. Ele retém 30 dias de dados de performance histórica de cinco minutos e 180 dias de dados de performance histórica de

uma hora. Isso permite que você visualize detalhes de desempenho muito granulares do mês atual e tendências gerais de desempenho por até um ano.

As pesquisas de coleta são compensadas por alguns minutos para que os dados de cada cluster não sejam enviados ao mesmo tempo, o que pode afetar o desempenho.

A tabela a seguir descreve as atividades de coleção executadas pelo Unified Manager:

<b>Atividade</b>	<b>Intervalo de tempo</b>	<b>Descrição</b>
Pesquisa de estatísticas de desempenho	A cada 5 minutos	Coleta dados de desempenho em tempo real de cada cluster.
Análise estatística	A cada 5 minutos	Após cada pesquisa de estatísticas, o Unified Manager compara os dados coletados com limites definidos pelo usuário, definidos pelo sistema e dinâmicos.  Se algum limite de desempenho tiver sido violado, o Unified Manager gerará eventos e enviará e-mails para usuários especificados, se configurado para fazê-lo.
Pesquisa de configuração	A cada 15 minutos	Coleta informações detalhadas de inventário de cada cluster para identificar todos os objetos de storage (nós, SVMs, volumes etc.).
Sumarização	A cada hora	Resume as mais recentes coleções de dados de desempenho de cinco minutos de 12 em médias horárias.  Os valores médios por hora são usados em algumas das páginas da IU e são retidos por 180 dias.
Análise de previsão e eliminação de dados	Todos os dias após a meia-noite	Analisa dados do cluster para estabelecer limites dinâmicos para latência de volume e IOPS nas próximas 24 horas.  Exclui do banco de dados quaisquer dados de desempenho de cinco minutos com mais de 30 dias.

Atividade	Intervalo de tempo	Descrição
Eliminação de dados	Todos os dias após as 2 da manhã	Exclui do banco de dados quaisquer eventos com mais de 180 dias e limites dinâmicos com mais de 180 dias.
Eliminação de dados	Todos os dias após as 3:30 da manhã	Exclui do banco de dados quaisquer dados de desempenho de uma hora com mais de 180 dias.

## O que é um ciclo de coleta de continuidade de dados

Um ciclo de coleta de continuidade de dados recupera dados de desempenho fora do ciclo de coleta de desempenho do cluster em tempo real que é executado, por padrão, a cada cinco minutos. As coletas de continuidade de dados permitem que o Unified Manager preencha lacunas de dados estatísticos que ocorrem quando não foi possível coletar dados em tempo real.

O Unified Manager realiza pesquisas de coleta de continuidade de dados de dados históricos de desempenho quando ocorrem os seguintes eventos:

- Inicialmente, um cluster é adicionado ao Unified Manager.

O Unified Manager reúne dados históricos de desempenho dos últimos 15 dias. Isso permite que você visualize duas semanas de informações históricas de desempenho de um cluster algumas horas após a sua adição.

Além disso, os eventos de limite definidos pelo sistema são reportados para o período anterior, se existirem.

- O ciclo de coleta de dados de desempenho atual não termina no tempo.

Se a pesquisa de desempenho em tempo real ultrapassar o período de coleta de cinco minutos, um ciclo de coleta de continuidade de dados é iniciado para reunir as informações ausentes. Sem a coleta de continuidade de dados, o próximo período de coleta é ignorado.

- O Unified Manager ficou inacessível por um período de tempo e depois ele volta a ficar on-line, como nas seguintes situações:
  - Foi reiniciado.
  - Ele foi desligado durante uma atualização de software ou ao criar um arquivo de backup.
  - Uma interrupção da rede é reparada.
- Um cluster ficou inacessível por um período de tempo e, em seguida, ele volta online, como nas seguintes situações:
  - Uma interrupção da rede é reparada.
  - Uma conexão de rede de área ampla lenta atrasou a coleta normal de dados de desempenho.

Um ciclo de coleta de continuidade de dados pode coletar no máximo 24 horas de dados históricos. Se o



Unified Manager estiver inativo por mais de 24 horas, uma lacuna nos dados de desempenho será exibida nas páginas da IU.

Um ciclo de coleta de continuidade de dados e um ciclo de coleta de dados em tempo real não podem ser executados ao mesmo tempo. O ciclo de coleta de continuidade de dados deve terminar antes que a coleta de dados de desempenho em tempo real seja iniciada. Quando a coleta de continuidade de dados for necessária para coletar mais de uma hora de dados históricos, você verá uma mensagem de banner para esse cluster na parte superior do painel notificações.

## O que significa o timestamp em dados e eventos coletados

O carimbo de data/hora que aparece nos dados de integridade e desempenho coletados, ou que aparece como hora de detecção de um evento, é baseado na hora do cluster do ONTAP, ajustada ao fuso horário definido no navegador da Web.

É altamente recomendável que você use um servidor NTP (Network Time Protocol) para sincronizar a hora em seus servidores Unified Manager, clusters ONTAP e navegadores da Web.



Se você vir carimbos de data/hora incorretos para um cluster específico, talvez queira verificar se a hora do cluster foi definida corretamente.

## Navegando em workflows de performance na GUI do Unified Manager

A interface do Unified Manager fornece muitas páginas para a coleta e exibição de informações de desempenho. Você usa o painel de navegação esquerdo para navegar para páginas na GUI e usa guias e links nas páginas para exibir e configurar informações.

Você usa todas as páginas a seguir para monitorar e solucionar problemas de informações de desempenho do cluster:

- página do painel de instrumentos
- páginas de inventário de objetos de armazenamento e rede
- páginas de detalhes do objeto de armazenamento (incluindo o explorador de desempenho)
- páginas de configuração e configuração
- páginas de eventos

## Iniciar sessão na IU

Você pode fazer login na IU do Unified Manager usando um navegador da Web compatível.

### Antes de começar

- O navegador da Web deve atender aos requisitos mínimos.

Consulte a Matriz de interoperabilidade em "[mysupport.NetApp.com/matrix](https://mysupport.netapp.com/matrix)" para obter a lista completa de versões de navegador suportadas.

- Você deve ter o endereço IP ou URL do servidor do Unified Manager.

Você será desconectado automaticamente da sessão após 1 hora de inatividade. Esse período de tempo pode ser configurado em **Geral > Configurações de recursos**.

### Passos

1. Digite o URL no navegador da Web, onde URL é o endereço IP ou nome de domínio totalmente qualificado (FQDN) do servidor do Unified Manager:
  - Para IPv4: `https://URL/`
  - Para IPv6: `https://[URL]/`

Se o servidor usar um certificado digital autoassinado, o navegador poderá exibir um aviso indicando que o certificado não é confiável. Você pode reconhecer o risco de continuar o acesso ou instalar um certificado digital assinado pela autoridade de certificação (CA) para autenticação do servidor. . No ecrã de início de sessão, introduza o seu nome de utilizador e palavra-passe.

Se o login na interface de usuário do Unified Manager estiver protegido usando autenticação SAML, você inserirá suas credenciais na página de login do provedor de identidade (IDP) em vez da página de login do Unified Manager.

É apresentada a página Painel de instrumentos.



Se o servidor do Unified Manager não for inicializado, uma nova janela do navegador exibirá o primeiro assistente de experiência. Você deve inserir um destinatário de e-mail inicial para o qual os alertas de e-mail serão enviados, o servidor SMTP que gerenciará as comunicações por e-mail e se o AutoSupport está habilitado para enviar informações sobre a instalação do Unified Manager para suporte técnico. A IU do Unified Manager é exibida depois que você preencher essas informações.

## Interface gráfica e caminhos de navegação

O Unified Manager tem grande flexibilidade e permite que você realize várias tarefas de várias maneiras. Há muitos caminhos de navegação que você descobrirá enquanto trabalha no Unified Manager. Embora nem todas as combinações possíveis de navegações possam ser mostradas, você deve estar familiarizado com alguns dos cenários mais comuns.

### Monitorar a navegação de objetos do cluster

Você pode monitorar o desempenho de todos os objetos em qualquer cluster gerenciado pelo Unified Manager. O monitoramento de seus objetos de storage fornece uma visão geral do desempenho do cluster e do objeto, além de incluir o monitoramento de eventos de desempenho. Você pode visualizar o desempenho e os eventos em um alto nível, ou você pode investigar mais detalhes sobre o desempenho do objeto e eventos de desempenho.

Este é um exemplo de muitas possíveis navegações de objetos de cluster:

1. Na página Dashboard, revise os detalhes no painel capacidade de desempenho para identificar o cluster que está usando a maior capacidade de performance e clique no gráfico de barras para navegar até a lista

de nós desse cluster.

2. Identifique o nó com o valor mais alto de capacidade de desempenho usado e clique nesse nó.
3. Na página nó / Explorador de desempenho, clique em **agregados neste nó** no menu Ver e comparar.
4. Identifique o agregado que está usando a maior capacidade de desempenho e clique nesse agregado.
5. Na página agregar / Explorador de desempenho, clique em **volumes neste agregado** no menu Exibir e comparar.
6. Identifique os volumes que estão usando a maioria das IOPS.

Você deve investigar esses volumes para ver se deve aplicar uma política de QoS ou uma política de nível de Serviço de Performance ou alterar as configurações de diretiva, de modo que esses volumes não usem uma porcentagem tão grande de IOPS no cluster.

**Dashboard** All Clusters

**Management Actions**

- Enable takeover on panic (2)
- Disable telnet (2)
- Enable volume autogrow (9)

**Capacity**

31 events (No new in past 24 hours)

CLUSTER	USED	DAYS TO FULL	REDUCTION
opm-sl...llicity	40.5 TB	< 1 month	13.0:1
umeng...1-02	83.6 TB	51 days	6.0:1
sysmgr...0-1-8	33 TB	149 days	8.3:1

**Performance Capacity**

No new events

CLUSTER	USED	DAYS TO FULL
umeng-aff220-01-02	83%	< 1 month
sysmgr-fas8060-1-8	49%	< 1 month
fas8040-206-21	46%	77 days

**Nodes** Last updated: Nov 15, 2019, 10:48 AM

VIEW Nodes on umeng-aff220-01-02 Search Nodes Filter Hardware Inventory Report

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Show/Hide

Status	Node	Latency	IOPS	MB/s	Performance Capacity Used	Utilization	Fr
✖	umeng-aff220-01	21.7 ms/op	27,333 IOPS	221 MB/s	73%	50%	3.1
✖	umeng-aff220-02	8.33 ms/op	83.4 IOPS	102 MB/s	53%	42%	6.1

**Node / Performance : umeng-aff220-01**

Summary Explorer Failover Planning Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Aggregates on this Node Filter

Aggregate	Latency	IOPS	MB/s	Perf...
NSLM12_002	12.4 ...	47.51...	5.6 M...	8%
NSLM12_001	11.4 ...	216 L...	4.33 ...	5%

**Aggregate / Performance : NSLM12\_002**

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Volumes on this Aggregate Filter

Volume	Latency	IOPS	MB/s
suchifa_vmaware_d...	6.38 ms...	76.8 IOPS	2.55 MB/s
suchifa_vmaware_d...	3.82 ms...	4,775 L...	18.7 MB/s
aiqum_scale_do_no...	0.114 m...	< 1 IOPS	< 1 MB/s

### Monitorar a navegação do desempenho do cluster

Você pode monitorar o desempenho de todos os clusters gerenciados pelo Unified Manager. O monitoramento dos clusters fornece uma visão geral do desempenho do cluster e do objeto, além de incluir o monitoramento de eventos de performance. Você pode visualizar o desempenho e os eventos em um alto nível ou investigar mais detalhes sobre eventos de desempenho e desempenho do cluster e do objeto.

Este é um exemplo de muitos caminhos de navegação possíveis de desempenho de cluster:

1. No painel de navegação à esquerda, clique em **Storage > Aggregates**.
2. Para exibir informações sobre o desempenho nesses agregados, selecione a visualização desempenho: Todos os agregados.
3. Identifique o agregado que você deseja investigar e clique nesse nome agregado para navegar para a página agregar/Explorador de desempenho.
4. Opcionalmente, selecione outros objetos para comparar com esse agregado no menu Exibir e comparar e, em seguida, adicione um dos objetos ao painel comparar.

As estatísticas para ambos os objetos aparecerão nos gráficos do contador para comparação.

5. No painel de comparação à direita na página Explorer, clique em **Zoom View** em um dos gráficos de contador para exibir detalhes sobre o histórico de desempenho desse agregado.

# Aggregates

Last updated: Nov 15, 2019, 1:18 PM

View: Performance: All Aggregates

Search Aggregates

Filter

Assign Performance Threshold Policy Clear Performance Threshold Policy

Scheduled Reports Show / Hide

Status	Aggregate	Type	Latency	IOPS	MB/s	Performance Capacity Used	Utilization
	aggr_evt	SSD	0.29 ms/op	3.79 IOPS	<1 MB/s	<1%	<1%
	aggr4	HDD	5.74 ms/op	14.4 IOPS	1.31 MB/s	6%	5%
	aggr3	HDD	5.06 ms/op	3.06 IOPS	<1 MB/s	6%	5%
	meg_aggr2	HDD	10.4 ms/op	52.9 IOPS	7.28 MB/s	3%	2%

## Aggregate / Performance : aggr4

Switch to Health View Last updated: Nov 15, 2019, 1:20 PM

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

TIME RANGE: Last 72 Hours

VIEW AND COMPARE: Aggregates on same Node

Filter

Aggregate	Late..Y	IOP...	MB/...	Perf...	
aggr3	5.06 ...	3.06 ...	<1 M...	6%	
aggr_evt	0.29 ...	3.79 ...	<1 M...	<1%	Add
aggr_automation	0.27...	8.35 ...	<1 M...	<1%	Add

Comparing 1 Additional Object

- aggr4
- aggr3

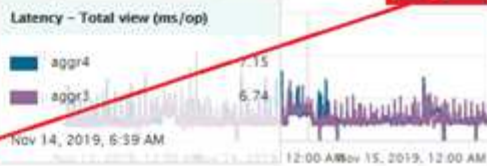
CHOOSE CHARTS: 7 Charts Selected

Events for Aggregate: aggr4

No data to display

Latency

view: Total Zoom View



## Latency for Aggregate: aggr4

Last updated: Nov 15, 2019, 1:23 PM

Event Timeline: aggr4

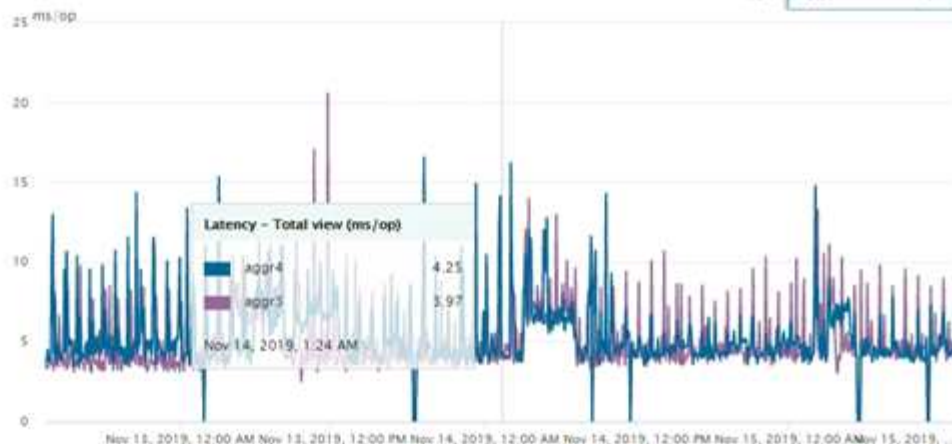
TIME RANGE: Last 72 Hours

- Critical Events
- Error Events
- Warning Events
- Information Events

No data to display

Comparing Objects

- aggr4
- aggr3



## Navegação de investigação de eventos

As páginas de detalhes do evento do Unified Manager fornecem uma visão detalhada de qualquer evento de desempenho. Isso é benéfico ao investigar eventos de desempenho, ao solucionar problemas e ao ajustar o desempenho do sistema.

Dependendo do tipo de evento de desempenho, você pode ver um dos dois tipos de páginas de detalhes do evento:

- Página de detalhes do evento para eventos de diretiva de limite definidos pelo usuário e definidos pelo sistema
- Página de detalhes do evento para eventos de política de limite dinâmico

Este é um exemplo de navegação de investigação de eventos.

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.
2. No menu Exibir, clique em **Eventos de desempenho ativo**.
3. Clique no nome do evento que você deseja investigar e a página de detalhes do evento será exibida.
4. Veja a Descrição do evento e reveja as ações sugeridas (quando disponíveis) para ver mais detalhes sobre o evento que podem ajudá-lo a resolver o problema. Você pode clicar no botão **Analyze Workload** para exibir gráficos de desempenho detalhados para ajudar a analisar o problema.

## Event Management

Last updated: Nov 15, 2019, 11:23 AM

Active performance events

Search Events



Filter

Assign To Acknowledge Mark as Resolved Add Alert

Show/Hide

Triggered Time	Severity	State	Impact Lev	Impact Area	Name	Source	Source Ty
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs2:/julia_feb12_vol3	Volume
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs7:/julia_non_shared_3	Volume
Nov 15, 2019, 5:04 AM	Warning	New	Risk	Performance	QoS volume Peak IOP... Threshold Breached	suchita_vmwarc...nt_delete_01	Volume
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency ... Service Level Policy	iscsi_boot/is.../ocum-c220-01	LUN
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency ... Service Level Policy	iscsi_boot/is.../ocum-c220-07	LUN

### Event: QoS Volume Peak IOPS/TB Warning Threshold Breached

(Last Seen: Nov 15, 2019, 11:19 AM)

IOPS value of 570 IOPS on policy group NSLM\_vs7\_Performance\_2\_0 has triggered a WARNING event to identify performance problems for the workloads in this policy group.



Actions

#### Suggested Actions to Fix The Issue

##### Troubleshoot

Analyze Workload

##### Take Action

This is an Adaptive QoS Policy that might be used by other workloads in the system.

If it is acceptable that changes you make to the QoS setting will be applied to other workloads that are using this policy,

- Increase the threshold to 4950 IOPS/TB for this Adaptive QoS Policy.

If you are satisfied with the current limitation on workload throughput

- Leave the QoS configuration setting as it is.

#### Event Information

EVENT TRIGGER TIME	SEVERITY	SOURCE
Nov 14, 2019, 11:39 AM	Warning	vs7:/julia_non_shared_3
STATE	IMPACT LEVEL	SOURCE TYPE
New	Risk	Volume
EVENT DURATION	IMPACT AREA	ON CLUSTER
1 day 40 minutes	Performance	ocum-mobility-01-02
LAST SEEN		AFFECTED OBJECTS COUNT
Nov 15, 2019, 11:19 AM		1
		TRIGGERED POLICY
		QoS Peak IOPS/TB threshold

## A procurar objetos de armazenamento

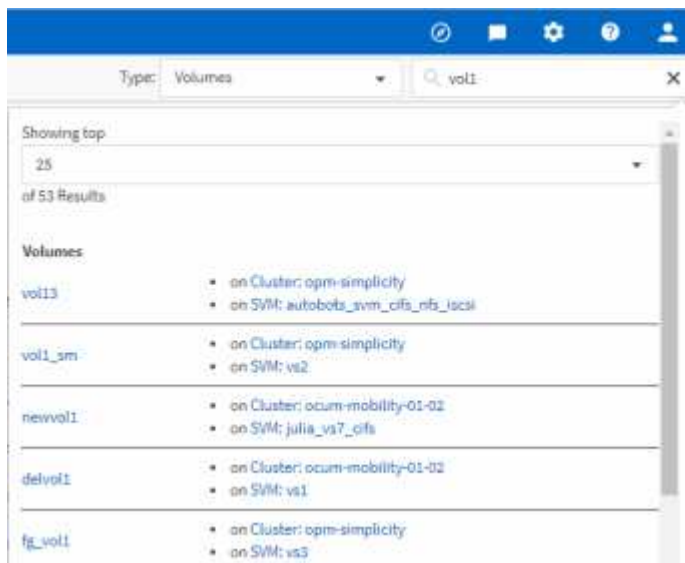
Para acessar rapidamente um objeto específico, você pode usar o campo **pesquisar todos os objetos de armazenamento** na parte superior da barra de menus. Este método de pesquisa global em todos os objetos permite localizar rapidamente objetos específicos por tipo. Os resultados da pesquisa são classificados por tipo de objeto de armazenamento e você pode filtrá-los usando o menu suspenso. Uma pesquisa válida deve conter pelo menos três caracteres.



A pesquisa global exibe o número total de resultados, mas apenas os 25 melhores resultados de pesquisa estão acessíveis. Por causa disso, a funcionalidade de pesquisa global pode ser considerada como uma ferramenta de atalho para encontrar itens específicos se você souber os itens que deseja localizar rapidamente. Para obter resultados de pesquisa completos, você pode usar a pesquisa nas páginas de inventário de objetos e sua funcionalidade de filtragem associada.

Você pode clicar na caixa suspensa e selecionar **All** para pesquisar simultaneamente todos os objetos e eventos. Alternativamente, você pode clicar na caixa suspensa para especificar o tipo de objeto. Digite um mínimo de três caracteres do nome do objeto ou evento no campo **pesquisar todos os objetos de armazenamento** e pressione **Enter** para exibir os resultados da pesquisa, como:

- Clusters: Nomes de cluster
- Nós: Nomes de nós
- Agregados: Nomes agregados
- SVMs: Nomes da SVM
- Volumes: Nomes de volumes
- LUNs: Caminhos LUN



LIFs e portas não são pesquisáveis na barra de pesquisa global.

Neste exemplo, a caixa suspensa tem o tipo de objeto volume selecionado. Digitar "vol" no campo **pesquisar todos os objetos de armazenamento** exibe uma lista de todos os volumes cujos nomes contêm esses caracteres. Para pesquisas de objetos, você pode clicar em qualquer resultado de pesquisa para navegar para a página do Performance Explorer desse objeto. Para pesquisas de eventos, clicar em um item no resultado da pesquisa navega para a página Detalhes do evento.

## Filtrando o conteúdo da página de inventário

Você pode filtrar os dados da página de inventário no Unified Manager para localizar rapidamente os dados com base em critérios específicos. Você pode usar a filtragem para restringir o conteúdo das páginas do Unified Manager para mostrar apenas os resultados nos quais você está interessado. Isso fornece um método muito eficiente de exibir apenas os dados nos quais você está interessado.

Use **Filtering** para personalizar a exibição de grade com base em suas preferências. As opções de filtro disponíveis são baseadas no tipo de objeto que está sendo visualizado na grade. Se os filtros forem aplicados atualmente, o número de filtros aplicados será exibido à direita do botão filtro.

Três tipos de parâmetros de filtro são suportados.

Parâmetro	Validação
Cadeia de caracteres (texto)	Os operadores são <b>contém</b> , <b>começa com</b> , <b>termina com</b> e <b>não contém</b> .
Número	Os operadores são <b>maiores que</b> , <b>menos que</b> , <b>no último</b> e <b>entre</b> .
Enum (texto)	Os operadores são <b>is</b> e <b>não</b> .

Os campos coluna, Operador e valor são necessários para cada filtro; os filtros disponíveis refletem as colunas filtráveis na página atual. O número máximo de filtros que você pode aplicar é de quatro. Os resultados filtrados são baseados em parâmetros de filtro combinados. Os resultados filtrados aplicam-se a todas as páginas da pesquisa filtrada, não apenas à página exibida atualmente.

Você pode adicionar filtros usando o painel filtragem.

1. Na parte superior da página, clique no botão **filtro**. O painel filtragem é exibido.
2. Clique na lista suspensa esquerda e selecione um objeto; por exemplo, *Cluster* ou um contador de desempenho.
3. Clique na lista pendente central e selecione o operador que pretende utilizar.
4. Na última lista, selecione ou insira um valor para concluir o filtro para esse objeto.
5. Para adicionar outro filtro, clique em *\* Adicionar filtro\**. É apresentado um campo de filtro adicional. Conclua este filtro usando o processo descrito nas etapas anteriores. Observe que ao adicionar seu quarto filtro, o botão *\* Adicionar filtro \** não é mais exibido.
6. Clique em **Apply Filter** (aplicar filtro). As opções de filtro são aplicadas à grade e o número de filtros é exibido à direita do botão filtro.
7. Use o painel filtragem para remover filtros individuais clicando no ícone de lixo à direita do filtro a ser removido.
8. Para remover todos os filtros, clique em **Reset** na parte inferior do painel de filtragem.

### Exemplo de filtragem

A ilustração mostra o painel filtragem com três filtros. O botão *\* Adicionar filtro \** é exibido quando você tem menos do que o máximo de quatro filtros.

MBps	greater than	5	MBps	
Node	name starts with	test		
Type	is	FCP Port		
+ Add Filter				
				<input type="button" value="Cancel"/> <input type="button" value="Apply Filter"/>

Depois de clicar em **Apply Filter**, o painel Filtering fecha, aplica os filtros e mostra o número de filtros aplicados ( 3 ).

## Monitoramento do desempenho do cluster no Dashboard

O Unified Manager Dashboard fornece alguns painéis que exibem o status de desempenho de alto nível de todos os clusters sendo monitorados por essa instância do Unified Manager. Ele permite avaliar o desempenho geral dos clusters gerenciados e anotar, localizar ou atribuir rapidamente para resolução quaisquer eventos específicos identificados.

### Compreender os painéis de desempenho no painel de instrumentos

O Unified Manager Dashboard fornece alguns painéis que exibem o status de desempenho de alto nível para todos os clusters que estão sendo monitorados no ambiente. Você pode optar por exibir o status de todos os clusters ou de um cluster individual.

Além de mostrar informações de desempenho, a maioria dos painéis também exibe o número de eventos ativos nessa categoria e o número de novos eventos adicionados nas 24 horas anteriores. Essas informações ajudam você a decidir quais clusters você pode precisar analisar mais para resolver eventos relatados. Clicar nos eventos exibe os principais eventos e fornece um link para a página de inventário do Gerenciamento de Eventos filtrada para mostrar os eventos nessa categoria.

Os painéis a seguir fornecem status de desempenho.

- **Painel de capacidade de desempenho**

Ao visualizar todos os clusters, esse painel exibe o valor da capacidade de desempenho para cada cluster (média sobre as 1 horas anteriores) e o número de dias até que a capacidade de desempenho atinja o limite superior (com base na taxa de crescimento diária). Clicar no gráfico de barras leva você à página de inventário de nós para esse cluster. Observe que a página de inventário de nós exibe a média da capacidade de desempenho nas 72 horas anteriores, portanto, esse valor pode não corresponder ao valor do Dashboard.

Ao exibir um único cluster, esse painel exibe a capacidade de desempenho do cluster, o total de IOPS e os valores de taxa de transferência total.

- **Painel de IOPS de carga de trabalho**

Quando o gerenciamento de workload ativo está ativado e, ao visualizar um único cluster, esse painel exibe o número total de workloads que estão atualmente em execução em um determinado intervalo de IOPS.

- **Painel de desempenho de carga de trabalho**

Quando o gerenciamento do workload ativo é ativado, esse painel exibe o número total de workloads em conformidade e não conformes atribuídos a cada nível de Serviço de Performance definido. Clicar em um gráfico de barras leva você às cargas de trabalho atribuídas a essa política na página cargas de trabalho.

- **Painel de visão geral de uso**

Ao visualizar todos os clusters, você pode optar por exibir clusters classificados por IOPS ou taxa de transferência mais alta (MB/s).

Ao visualizar um único cluster, você pode optar por exibir workloads nesse cluster classificados por IOPS ou taxa de transferência mais alta (MB/s).

## Mensagens de banner de desempenho e descrições

O Unified Manager pode exibir mensagens de banner na página notificações (no sino de notificação) para alertá-lo sobre problemas de status de um cluster específico.

Mensagem de banner	Descrição	Resolução
No performance data is being collected from cluster <i>cluster_name</i> . Restart Unified Manager to correct this issue.	O serviço de coleta do Unified Manager parou e nenhum dado de performance está sendo coletado de clusters.	Reinicie o Unified Manager para corrigir esse problema. Se isso não corrigir o problema, entre em Contato com o suporte técnico.
More than x hour(s) of historical data is being collected from cluster <i>cluster_name</i> . Current data collections will start after all historical data is collected.	Um ciclo de coleta de continuidade de dados está sendo executado atualmente para recuperar dados de desempenho fora do ciclo de coleta de desempenho do cluster em tempo real.	Nenhuma ação é necessária. Os dados de desempenho atuais serão recolhidos após a conclusão do ciclo de recolha da continuidade dos dados.  Um ciclo de coleta de continuidade de dados é executado quando um novo cluster é adicionado ou quando o Unified Manager não conseguiu coletar dados de desempenho atuais por algum motivo.

## Alterar o intervalo de coleta de estatísticas de desempenho

O intervalo de coleta padrão para estatísticas de desempenho é de 5 minutos. Você pode alterar esse intervalo para 10 ou 15 minutos se achar que coleções de clusters grandes não estão finalizadas dentro do tempo padrão. Essa configuração afeta a coleção de estatísticas de todos os clusters que essa instância do Unified Manager está

monitorando.

### Antes de começar

Você deve ter uma ID de usuário e senha autorizados para fazer login no console de manutenção do servidor do Unified Manager.

A emissão de coleções de estatísticas de desempenho que não terminam no prazo é indicada pelas mensagens de banner `Unable to consistently collect from cluster <cluster_name>` ou `Data collection is taking too long on cluster <cluster_name>`.

Você deve alterar o intervalo de coleta somente quando necessário devido a um problema de coleta de estatísticas. Não altere esta definição por qualquer outro motivo.



Alterar esse valor da configuração padrão de 5 minutos pode afetar o número e a frequência dos eventos de desempenho reportados pelo Unified Manager. Por exemplo, os limites de desempenho definidos pelo sistema acionam eventos quando a política é excedida por 30 minutos. Ao usar coleções de 5 minutos, a política deve ser excedida por seis coleções consecutivas. Para coleções de 15 minutos, a política deve ser excedida por apenas dois períodos de coleta.

Uma mensagem na parte inferior da página Configuração do cluster indica o intervalo de coleta de dados estatísticos atual.

### Passos

1. Faça login usando SSH como o usuário de manutenção no host do Unified Manager.

Os prompts do console de manutenção do Unified Manager são exibidos.

2. Digite o número da opção de menu chamada **Configuração do intervalo de polling de desempenho** e pressione Enter.
3. Se solicitado, digite a senha do usuário de manutenção novamente.
4. Digite o número do novo intervalo de polling que deseja definir e pressione Enter.


Se você alterou o intervalo de coleta do Unified Manager para 10 ou 15 minutos e tiver uma conexão atual com um provedor de dados externo (como Graphite), altere o intervalo de transmissão do provedor de dados para que ele seja igual ou maior que o intervalo de coleta do Unified Manager.

## Solução de problemas de cargas de trabalho usando o analisador de carga de trabalho

O analisador de carga de trabalho fornece uma maneira de visualizar critérios importantes de integridade e desempenho para uma única carga de trabalho em uma única página para ajudar na solução de problemas. Ao visualizar todos os eventos atuais e passados para um workload, você pode ter uma ideia melhor por que o workload pode estar tendo um problema de performance ou capacidade agora.

O uso dessa ferramenta também pode ajudá-lo a determinar se o armazenamento é a causa de quaisquer problemas de desempenho de um aplicativo ou se o problema é causado por uma rede ou outro problema relacionado.

Você pode iniciar essa funcionalidade a partir de uma variedade de locais na interface do usuário:

- A partir da seleção análise de carga de trabalho no menu de navegação à esquerda
- Na página de detalhes do evento clicando no botão **Analyze Workload**
- A partir de qualquer página de inventário de carga de trabalho (volume, LUN, carga de trabalho, partilha NFS ou partilha SMB/CIFS), clicando no ícone mais  e, em seguida, em **analisar carga de trabalho**
- Na página máquinas virtuais, clicando no botão **Analyze Workload** de qualquer objeto de datastore

Ao iniciar a ferramenta no menu de navegação à esquerda, você pode inserir o nome de qualquer carga de trabalho que deseja analisar e selecionar o intervalo de tempo para o qual deseja solucionar problemas. Quando você inicia a ferramenta a partir de qualquer uma das páginas de inventário de carga de trabalho ou máquina virtual, o nome da carga de trabalho é preenchido automaticamente e os dados da carga de trabalho são apresentados com o intervalo de tempo padrão de 2 horas. Quando você inicia a ferramenta na página de detalhes do evento, o nome da carga de trabalho é preenchido automaticamente e os dados de 10 dias são exibidos.

## Quais dados o analisador de carga de trabalho exibe

A página do analisador de carga de trabalho exibe informações sobre quaisquer eventos atuais que possam estar afetando a carga de trabalho, recomendações para corrigir potencialmente o problema que causa o evento e gráficos para analisar o histórico de desempenho e capacidade.

Na parte superior da página, você especifica o nome da carga de trabalho (volume ou LUN) que deseja analisar e o período de tempo sobre o qual deseja ver as estatísticas. Você pode alterar o período de tempo a qualquer momento, se quiser ver um período de tempo mais curto ou mais longo.

As outras áreas da página exibem os resultados da análise e os gráficos de desempenho e capacidade.



Os gráficos de workload de LUNs não fornecem o mesmo nível de estatísticas que os gráficos de volumes. Assim, você notará diferenças ao analisar esses dois tipos de workloads.

### • Área de resumo de eventos

Exibe uma breve visão geral do número e tipos de eventos que ocorreram durante o período de tempo. Quando há eventos de diferentes áreas de impactos (por exemplo, desempenho e capacidade), essas informações são exibidas para que você possa selecionar detalhes para o tipo de evento em que você está interessado. Clique no tipo de evento para exibir uma lista dos nomes dos eventos.

Se houver apenas um evento durante o período de tempo, uma lista de recomendações para corrigir o problema será listada para alguns eventos.

### • Linha do tempo do evento

Mostra todas as ocorrências de eventos durante o período de tempo especificado. Passe o cursor sobre cada evento para ver o nome do evento.

Se você chegou a esta página clicando no botão **Analyze Workload** na página de detalhes do evento, o ícone do evento selecionado aparece maior para que você possa identificar o evento.

### • Área dos gráficos de desempenho

Exibe gráficos de latência, taxa de transferência (IOPS e MB/s) e utilização (para o nó e agregado) com base no período de tempo selecionado. Você pode clicar no link Exibir detalhes de desempenho para

exibir a página do Performance Explorer para a carga de trabalho, caso queira realizar análises adicionais.

- **Latência** exibe a latência da carga de trabalho no período de tempo selecionado. O gráfico tem três visualizações que permitem ver:

- **Latência total**
- **Breakdown** latência (dividido por leituras, gravações e outros processos)
- \* Latência de componentes de cluster\* (dividido por componente de cluster)

"Componentes do cluster e por que eles podem estar na contenção" Consulte para obter uma descrição dos componentes do cluster que são apresentados aqui. **Throughput exibe IOPS e MB/s throughput para a carga de trabalho no período selecionado. O gráfico tem quatro visualizações que permitem ver: \* Taxa de transferência total \* taxa de transferência detalhada (dividida por leituras, gravações e outros processos) \* taxa de transferência em nuvem** (os MB/s que estão sendo usados para gravar dados e ler dados da nuvem; para aquelas cargas de trabalho que estão em camadas de capacidade para a nuvem) \* **com previsão (uma previsão do que os valores de taxa de taxa de transferência mínima, se você também pode ser configurados para o limite de tempo de taxa de taxa de transferência).** **Utilização** exibe a utilização tanto para o agregado quanto para o nó em que a carga de trabalho está sendo executada durante o período de tempo selecionado. A partir daqui, você pode ver se seu agregado ou nó está sobreutilizado, possivelmente causando alta latência. Ao analisar volumes do FlexGroup, há vários nós e agregados listados nos gráficos de utilização.

- \* Área do gráfico de capacidade\*

Exibe gráficos para capacidade de dados e capacidade Snapshot do último mês para o workload.

Para volumes, você pode clicar no link Exibir detalhes da capacidade para exibir a página Detalhes de integridade da carga de trabalho, caso queira realizar análises adicionais. Os LUNs não fornecem esse link porque não há página de Detalhes de integridade para LUNs.

- **Capacity View** exibe o espaço disponível total alocado para a carga de trabalho e o espaço lógico usado (após todas as otimizações do NetApp).
- **Exibição Snapshot** exibe o espaço total reservado para cópias Snapshot e a quantidade de espaço atualmente sendo usado. Observe que os LUNs não fornecem uma Exibição Snapshot.
- **O Cloud Tier View** exibe a quantidade de capacidade que está sendo usada no nível de desempenho local e a quantidade que está sendo usada no nível de nuvem. Esses gráficos incluem uma estimativa do tempo restante antes que a capacidade esteja cheia para essa carga de trabalho. Esta informação baseia-se no uso histórico e requer um mínimo de 10 dias de dados. Quando restam menos de 30 dias de capacidade, o Unified Manager identifica o storage como "quase cheio".


## Quando eu usaria o analisador da carga de trabalho

Normalmente, você usaria o analisador de carga de trabalho para solucionar um problema de latência relatado por um usuário, para analisar mais detalhadamente um evento ou alerta relatado ou para explorar uma carga de trabalho que você vê estar operando de forma anormal.

No caso de os usuários contatarem você para dizer que o aplicativo que estão usando está sendo executado muito lentamente, você pode verificar os gráficos de latência, taxa de transferência e utilização da carga de trabalho sobre a qual o aplicativo está sendo executado para ver se o storage é a causa do problema de performance. Você também pode usar o gráfico de capacidade para ver se a capacidade é baixa porque um sistema ONTAP no qual a capacidade é superior a 85% usado pode causar problemas de desempenho. Esses gráficos ajudarão você a determinar se o problema é causado pelo armazenamento ou por uma rede

ou outro problema relacionado.

No caso de o Unified Manager gerar um evento de desempenho e desejar analisar a causa do problema com mais profundidade, você pode iniciar o analisador de carga de trabalho na página de detalhes do evento clicando no botão **Analyze Workload** para pesquisar algumas das tendências de latência, taxa de transferência e capacidade da carga de trabalho.

No caso de você notar uma carga de trabalho que parece estar operando anormalmente ao visualizar qualquer página de inventário de carga de trabalho (volume, LUN, carga de trabalho, compartilhamento NFS ou compartilhamento SMB/CIFS), você pode clicar no ícone mais  e depois em **analisar carga de trabalho** para abrir a página análise de carga de trabalho para examinar a carga de trabalho ainda mais.

## Usando o analisador de carga de trabalho

Há muitas maneiras de iniciar o analisador de carga de trabalho a partir da interface do usuário. Aqui descrevemos o lançamento da ferramenta a partir do painel de navegação à esquerda.

### Passos

1. No painel de navegação esquerdo, clique em **análise de carga de trabalho**.

É apresentada a página análise de carga de trabalho.

2. Se souber o nome da carga de trabalho, introduza o nome. Se você não tiver certeza do nome completo, insira um mínimo de 3 caracteres e o sistema exibirá uma lista de cargas de trabalho que correspondem à cadeia de caracteres.
3. Selecione o intervalo de tempo se pretender ver estatísticas durante mais de 2 horas e clique em **Apply** (aplicar).
4. Visualize a área Resumo para ver os eventos que ocorreram durante o período de tempo.
5. Visualize os gráficos de desempenho e capacidade para ver quando qualquer uma das métricas está anormal e veja se algum evento está alinhado com a entrada anormal.

## Monitoramento do desempenho do cluster na página de destino do cluster de desempenho

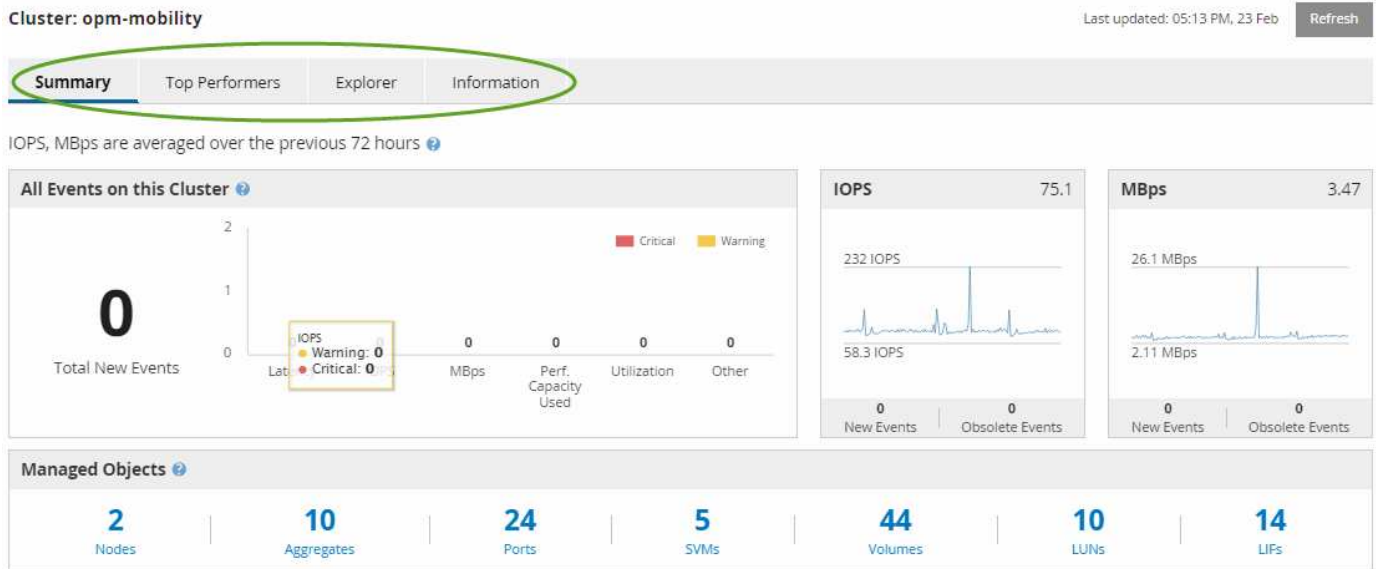
A página de destino do cluster de desempenho exibe o status de desempenho de alto nível de um cluster selecionado que está sendo monitorado por uma instância do Unified Manager. Esta página permite avaliar o desempenho geral de um cluster específico e anotar, localizar ou atribuir rapidamente para resolução quaisquer eventos específicos de cluster identificados.

### Compreender a página de destino do cluster de desempenho

A página de destino do cluster de desempenho fornece uma visão geral de desempenho de alto nível de um cluster selecionado, com ênfase no status de desempenho dos 10 principais objetos dentro do cluster. Os problemas de desempenho são exibidos na parte superior da página, no painel todos os eventos neste cluster.



A página de destino do cluster de desempenho fornece uma visão geral de alto nível de cada cluster gerenciado por uma instância do Unified Manager. Esta página fornece informações sobre eventos e performance, além de permitir que você monitore e solucione problemas de clusters. A imagem a seguir mostra um exemplo da página de destino do cluster de desempenho para o cluster chamado opm-mobility:



A contagem de eventos na página Resumo do cluster pode não corresponder à contagem de eventos na página Inventário de Eventos de desempenho. Isso ocorre porque a página Resumo do cluster pode mostrar um evento cada nas barras de latência e utilização quando as políticas de limite de combinação foram violadas, enquanto a página Inventário de Eventos de desempenho mostra apenas um evento quando uma diretiva de combinação foi violada.



Se um cluster foi removido de ser gerenciado pelo Unified Manager, o status **removido** é exibido à direita do nome do cluster na parte superior da página.

## Página inicial do cluster de desempenho

A página de destino do cluster de desempenho exibe o status de desempenho de alto nível de um cluster selecionado. A página permite acessar detalhes completos de cada contador de desempenho para os objetos de armazenamento no cluster selecionado.

A página de destino do cluster de desempenho inclui quatro guias que separam os detalhes do cluster em quatro áreas de informações:

- Página de resumo
  - Painel Eventos do cluster
  - Gráficos de desempenho de MB/s e IOPS
  - Painel objetos gerenciados
- Página de melhores performers
- Página Explorer
- Página de informações

## Página Resumo do cluster de performance

A página Resumo do cluster de desempenho fornece um resumo dos eventos ativos, desempenho do IOPS e desempenho de MB/s de um cluster. Esta página também inclui a contagem total dos objetos de armazenamento no cluster.

### Painel de eventos de desempenho do cluster

O painel de eventos de desempenho do cluster exibe estatísticas de desempenho e todos os eventos ativos do cluster. Isso é mais útil quando você monitora seus clusters e todos os eventos e performance relacionados ao cluster.

### Todos os eventos neste painel de cluster

O painel todos os eventos neste cluster exibe todos os eventos de desempenho do cluster ativo para as 72 horas anteriores. O total de eventos ativos é exibido à esquerda; esse número representa o total de todos os eventos novos e reconhecidos para todos os objetos de armazenamento neste cluster. Você pode clicar no link [Eventos ativos totais](#) para navegar até a página [Inventário de Eventos](#), que é filtrada para exibir esses eventos.

O gráfico de barras **Total ative Events** (Eventos ativos totais) do cluster apresenta o número total de eventos críticos e de aviso ativos:

- Latência (total para nós, agregados, SVMs, volumes, LUNs e namespaces)
- IOPS (total de clusters, nós, agregados, SVMs, volumes, LUNs e namespaces)
- MB/s (total de clusters, nós, agregados, SVMs, volumes, LUNs, namespaces, portas e LIFs)
- Capacidade de performance utilizada (total para nós e agregados)
- Utilização (total de nós, agregados e portas)
- Outro (taxa de falta de cache para volumes)

A lista contém eventos de desempenho ativos acionados por políticas de limite definidas pelo usuário, políticas de limite definidas pelo sistema e limites dinâmicos.

Os dados do gráfico (barras do contador vertical) são exibidos em vermelho (■) para eventos críticos e amarelo (■) para eventos de aviso. Posicione o cursor sobre cada barra do contador vertical para visualizar o tipo e o número reais de eventos. Você pode clicar em **Refresh** para atualizar os dados do painel do contador.

Você pode mostrar ou ocultar eventos críticos e de aviso no gráfico de desempenho **Total ative Events** clicando nos ícones **Critical** e **Warning** na legenda. Se ocultar determinados tipos de eventos, os ícones de legenda são apresentados a cinzento.

### Contra-painéis

Os painéis do contador exibem eventos de atividade e desempenho do cluster para as 72 horas anteriores e incluem os seguintes contadores:

- **Painel do contador de IOPS**

IOPS indica a velocidade de operação do cluster em número de operações de entrada/saída por segundo. Este painel do contador fornece uma visão geral de alto nível da integridade do IOPS do cluster para o período de 72 horas anterior. Você pode posicionar o cursor sobre a linha de tendência do gráfico para

exibir o valor de IOPS para um tempo específico.

- \* Painel do contador MB/s\*

MB/s indica a quantidade de dados transferidos de e para o cluster em megabytes por segundo. Este painel do contador fornece uma visão geral de alto nível da integridade MB/s do cluster para o período de 72 horas anterior. Você pode posicionar o cursor sobre a linha de tendência do gráfico para exibir o valor MB/s para um tempo específico.

O número no canto superior direito do gráfico na barra cinza é o valor médio do último período de 72 horas. Os números mostrados na parte inferior e superior do gráfico de linhas de tendência são os valores mínimo e máximo para o último período de 72 horas. A barra cinza abaixo do gráfico contém a contagem de eventos ativos (novos e reconhecidos) e eventos obsoletos do último período de 72 horas.

Os painéis do contador contêm dois tipos de eventos:

- **Ativo**

Indica que o evento de desempenho está ativo no momento (novo ou confirmado). O problema que causa o evento não foi corrigido ou não foi resolvido. O contador de performance do objeto de storage permanece acima do limite de performance.

- **Obsoleto**

Indica que o evento já não está ativo. O problema que causa o evento foi corrigido ou foi resolvido. O contador de desempenho do objeto de storage não está mais acima do limite de desempenho.

Para **Eventos ativos**, se houver um evento, você pode posicionar o cursor sobre o ícone do evento e clicar no número do evento para vincular à página Detalhes do evento apropriada. Se houver mais de um evento, você pode clicar em **Exibir todos os eventos** para exibir a página Inventário de Eventos, que é filtrada para mostrar todos os eventos para o tipo de contador de objetos selecionado.

### Painel objetos gerenciados

O painel objetos gerenciados na guia Resumo de desempenho fornece uma visão geral de nível superior dos tipos e contagens de objetos de storage para o cluster. Esse painel permite rastrear o status dos objetos em cada cluster.

A contagem de objetos gerenciados é de dados pontuais a partir do último período de coleta. Novos objetos são descobertos em intervalos de 15 minutos.

Clicar no número vinculado para qualquer tipo de objeto exibe a página de inventário de desempenho do objeto para esse tipo de objeto. A página de inventário de objetos é filtrada para mostrar apenas os objetos neste cluster.

Os objetos gerenciados são:

- \* Nós\*

Um sistema físico em um cluster.

- **Agregados**

Um conjunto de vários grupos de matriz redundante de discos independentes (RAID) que podem ser

gerenciados como uma única unidade para proteção e provisionamento.

- **Portos**

Um ponto de conexão físico em nós que é usado para se conectar a outros dispositivos em uma rede.

- **Storage VMs**

Uma máquina virtual que fornece acesso à rede através de endereços de rede exclusivos. Um SVM pode servir dados a partir de um namespace distinto e pode ser administrado separadamente do resto do cluster.

- **Volumes**

Uma entidade lógica que contém dados de usuário acessíveis por meio de um ou mais protocolos de acesso suportados. A contagem inclui volumes FlexVol e volumes FlexGroup; ela não inclui componentes do FlexGroup.

- **LUNs**

O identificador de uma unidade lógica Fibre Channel (FC) ou de uma unidade lógica iSCSI. Uma unidade lógica normalmente corresponde a um volume de armazenamento e é representada dentro de um sistema operacional de computador como um dispositivo.

- \* Interfaces de rede\*

Uma interface de rede lógica que representa um ponto de acesso à rede para um nó. A contagem inclui todos os tipos de interface.

## **Página de melhores performers**

A página principais executores exibe os objetos de armazenamento que têm o desempenho mais alto ou o desempenho mais baixo, com base no contador de desempenho selecionado. Por exemplo, na categoria VMs de armazenamento, você pode exibir os SVMs que têm o IOPS mais alto, a latência mais alta ou os MB/s. mais baixos Esta página também mostra se algum dos melhores artistas tem algum evento de desempenho ativo (novo ou reconhecido).

A página Top Performers exibe um máximo de 10 de cada objeto. Observe que o objeto volume inclui volumes FlexVol e volumes FlexGroup.

- **Intervalo de tempo**

Pode selecionar um intervalo de tempo para visualizar os melhores desempenhos; o intervalo de tempo selecionado aplica-se a todos os objetos de armazenamento. Intervalos de tempo disponíveis:

- Hora da última
- Últimas 24 horas
- Últimas 72 horas (padrão)
- Últimos 7 dias

- **Métrica**

Clique no menu **Metric** para selecionar um contador diferente. As opções de contador são exclusivas do tipo de objeto. Por exemplo, os contadores disponíveis para o objeto **volumes** são **latência**, **IOPS** e **MB/s**. Alterar o contador recarrega os dados do painel com os melhores desempenhos com base no contador selecionado.

Contadores disponíveis:

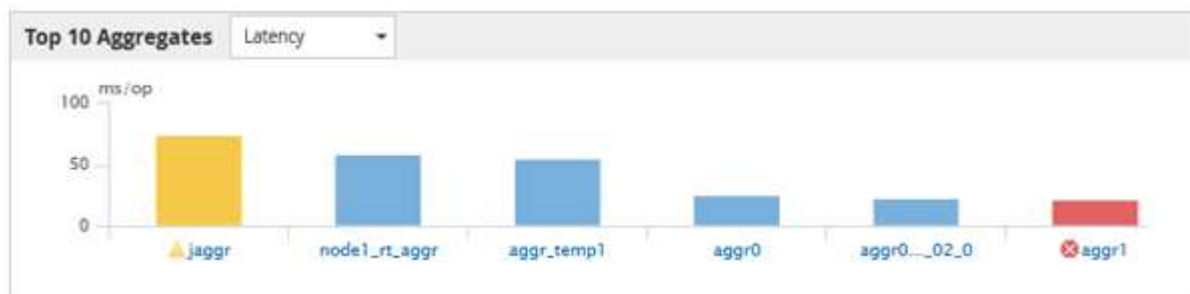
- Latência
- IOPS
- MB/s
- Capacidade de performance utilizada (para nós e agregados)
- Utilização (para nós e agregados)

#### • Ordenar

Clique no menu **Classificar** para selecionar uma classificação ascendente ou descendente para o objeto e contador selecionados. As opções são **mais altas a mais baixas** e **mais baixas a mais altas**. Essas opções permitem que você visualize os objetos com o desempenho mais alto ou o menor desempenho.

#### • Barra de contador

A barra de contador no gráfico mostra as estatísticas de desempenho para cada objeto, representadas como uma barra para esse item. Os gráficos de barras são codificados por cores. Se o contador não estiver a violar um limite de desempenho, a barra do contador é apresentada a azul. Se uma violação de limite estiver ativa (um evento novo ou confirmado), a barra será exibida na cor do evento: Os eventos de aviso são exibidos em amarelo (■) e os eventos críticos são exibidos em vermelho (■). As violações de limite são mais indicadas pelos ícones do indicador de eventos de gravidade para avisos e eventos críticos.



Para cada gráfico, o eixo X exibe os melhores desempenhos para o tipo de objeto selecionado. O eixo Y exibe as unidades aplicáveis ao contador selecionado. Clicar no link do nome do objeto abaixo de cada elemento de gráfico de barras vertical navega para a página de destino de desempenho do objeto selecionado.

#### • Indicador de evento de gravidade

O ícone do indicador **evento de gravidade** é exibido à esquerda de um nome de objeto para eventos críticos ativos (⊗) ou de aviso (⚠) nos gráficos com desempenho superior. Clique no ícone do indicador **evento de gravidade** para visualizar:

- **Um evento**

Navega para a página de detalhes do evento para esse evento.

- **Dois ou mais eventos**

Navega para a página de inventário de eventos, que é filtrada para exibir todos os eventos para o objeto selecionado.

- **Botão Exportar**


Cria um `.csv` arquivo que contém os dados que aparecem na barra do contador. Você pode optar por criar o arquivo para o único cluster que está visualizando ou para todos os clusters no data center.

## Monitorando o desempenho usando as páginas Inventário de desempenho

As páginas de desempenho de inventário de objetos exibem informações de desempenho, eventos de desempenho e integridade de objetos para todos os objetos dentro de uma categoria de tipo de objeto. Isso fornece uma visão geral do status de performance de cada objeto em um cluster, por exemplo, para todos os nós ou todos os volumes.





As páginas de desempenho de inventário de objetos fornecem uma visão geral de alto nível do status do objeto, permitindo que você avalie o desempenho geral de todos os objetos e compare os dados de desempenho do objeto. Você pode refinar o conteúdo das páginas de inventário de objetos pesquisando, classificando e filtrando. Isso é benéfico ao monitorar e gerenciar o desempenho do objeto, pois permite localizar rapidamente objetos com problemas de desempenho e iniciar o processo de solução de problemas.

Nodes - Performance / All Nodes 

Last updated: Jan 17, 2019, 7:54 AM 

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

View All Nodes  

<input type="checkbox"/>	Status	Node	Latency	IOPS	MBps	Flash Cache Reads	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster
<input type="checkbox"/>		ocum-mobility-02	10.2 ms/op	18,884 IOPS	156 MBps	N/A	81%	35%	16.6 TB	23.2 TB	ocum-mobility-01-02
<input checked="" type="checkbox"/>		opm-simplicity-01	2.01 ms/op	39,358 IOPS	153 MBps	< 1%	119%	88%	4.88 TB	18.3 TB	opm-simplicity
<input type="checkbox"/>		ocum-mobility-01	0.018 ms/op	< 1 IOPS	18.2 MBps	N/A	23%	18%	8.69 TB	15.7 TB	ocum-mobility-01-02
<input type="checkbox"/>		opm-simplicity-02	17 ms/op	14,627 IOPS	124 MBps	< 1%	29%	20%	212 GB	5.88 TB	opm-simplicity

Por padrão, os objetos nas páginas de inventário de desempenho são classificados com base na criticidade de desempenho do objeto. Os objetos com novos eventos críticos de desempenho são listados primeiro e os objetos com eventos de aviso são listados em segundo lugar. Isso fornece uma indicação visual imediata dos problemas que devem ser resolvidos. Todos os dados de performance são baseados em uma média de 72 horas.

Você pode navegar facilmente da página de desempenho do inventário de objetos para uma página de detalhes do objeto clicando no nome do objeto na coluna Nome do objeto. Por exemplo, na página de inventário desempenho/todos os nós, você clicaria em um objeto de nó na coluna **nós**. A página de detalhes do objeto fornece informações detalhadas e detalhes sobre o objeto selecionado, incluindo comparação lado a lado de eventos ativos.

## Exibindo páginas de inventário de desempenho para todos os objetos de armazenamento

Use as páginas de inventário de desempenho para ver um resumo das informações de performance sobre cada um dos objetos de storage disponíveis, como clusters, agregados, volumes, etc. Você pode vincular as páginas de detalhes do objeto Performance para exibir informações detalhadas de um objeto específico.

Por padrão, os objetos nas páginas de visualização são classificados com base na criticidade do evento. Os objetos com eventos críticos são listados primeiro e os objetos com eventos de aviso são listados em segundo lugar. Isso fornece uma indicação visual imediata dos problemas que devem ser resolvidos.

Você pode exportar dados dessas páginas para um (.csv`arquivo de valores separados por vírgula ), arquivo do Microsoft Excel (.xlsx`) ou (.pdf`documento ) usando o botão **relatórios** e, em seguida, usar os dados exportados para criar relatórios. Além disso, você pode personalizar a página e, em seguida, agendar um relatório para ser criado e enviado por e-mail regularmente usando o botão **relatórios programados**.

Todos os campos nessas páginas podem ser usados em visualizações personalizadas e em relatórios. Alguns dos campos estão ligados a páginas relacionadas, permitindo uma visualização mais detalhada.

### Desempenho: Visualização de todos os clusters

A exibição desempenho: Todos os clusters exibe uma visão geral dos eventos de desempenho, dados e informações de configuração de cada cluster monitorado por uma instância do Unified Manager. Essa página permite monitorar a performance dos clusters e solucionar problemas de performance e eventos de limite.

Você pode atribuir políticas de limite de desempenho ou limpar políticas de limite de qualquer objeto nas páginas de inventário de objetos usando os botões **atribuir política de limite de desempenho** e **Limpar política de limite de desempenho**.

A seguir estão alguns campos importantes na exibição desempenho: Todos os clusters.

- Cluster FQDN: O nome de domínio totalmente qualificado (FQDN) do cluster.
- IOPS: As operações de entrada/saída por segundo no cluster.
- MB/s: A taxa de transferência no cluster, medida em MIB por segundo.
- Campos de capacidade: Capacidade livre e total em GiB.
- Nome do host ou endereço IP: O nome do host ou endereço IP (IPv4 ou IPv6) do LIF de gerenciamento de cluster.
- Versão DO SO: A versão do software ONTAP instalada no cluster.




Se forem instaladas versões diferentes do software ONTAP nos nós do cluster, o número de versão mais baixo será listado. É possível exibir a versão do ONTAP instalada em cada nó na exibição desempenho: Todos os nós.

- Política de limite: A política de limite de desempenho definido pelo usuário, ou políticas, que estão ativas neste objeto de storage. Você pode posicionar o cursor sobre os nomes de políticas que contêm uma elipse (...) para exibir o nome completo da política ou a lista de nomes de políticas atribuídos. Os botões Assign Performance Threshold Policy e Clear Performance Threshold Policy permanecem desabilitados até que você selecione um ou mais objetos clicando nas caixas de seleção localizadas à esquerda.

## Performance: Visualização de todos os volumes

A exibição desempenho: Todos os volumes exibe uma visão geral dos eventos de performance, dados de contador e informações de configuração de cada volume do FlexVol volume e do FlexGroup que está sendo monitorado por uma instância do Unified Manager. Isso permite que você monitore rapidamente a performance dos volumes e solucione problemas de performance e eventos de limite.

Para analisar a latência e a taxa de transferência de um objeto específico, clique no botão mais opções  e depois em **analisar carga de trabalho** e você pode visualizar gráficos de desempenho e capacidade na página análise de carga de trabalho. Você pode ver os detalhes no System Manager, desde que você tenha credenciais válidas para o System Manager.



Para volumes de proteção de dados (DP), somente os valores de contador para tráfego gerado pelo usuário são exibidos. Os volumes raiz não são exibidos nesta página.

A seguir estão alguns campos importantes na exibição desempenho: Todos os volumes.

- Estilo: FlexVol ou FlexGroup.
- Latência: Para volumes FlexVol, esse é o tempo médio de resposta do volume para todas as solicitações de e/S, expresso em milissegundos por operação. Para volumes FlexGroup, essa é a latência média de todos os volumes constituintes.
- IOPS/TB: O número de operações de entrada/saída processadas por segundo com base no espaço total que está sendo consumido pela carga de trabalho, em terabytes. Este contador mede quanto desempenho pode ser entregue por uma determinada quantidade de capacidade de armazenamento.
- IOPS: Para volumes FlexVol, esse é o número de operações de entrada/saída por segundo para o volume. Para volumes FlexGroup, essa é a soma de IOPS para todos os volumes constituintes.
- MB/s: Para volumes FlexVol, esta é a taxa de transferência no volume, medida em megabytes por segundo. Para volumes FlexGroup, esta é a soma de MB/s para todos os volumes constituintes.
- Campos de capacidade: Capacidade livre e total em GiB.

Consulte os links a seguir para obter mais informações:

- ["Atribuindo políticas de limite de desempenho a objetos de storage"](#)
- ["Remoção de políticas de limite de performance de objetos de storage"](#)
- ["Tipos de workloads monitorados pelo Unified Manager"](#)
- ["Exibindo as configurações do grupo de políticas de QoS aplicadas a volumes ou LUNs específicos"](#)
- ["Compreensão das recomendações do Unified Manager para categorizar dados na nuvem"](#)
- ["Exibição de gráficos de desempenho para comparar volumes ou LUNs que estão no mesmo grupo de políticas de QoS"](#)

## Performance: Visualização de todos os agregados

A visualização desempenho: Todos os agregados exibe uma visão geral dos eventos de performance, dados e informações de configuração de cada agregado monitorado por uma instância do Unified Manager. Essa página permite monitorar a performance de agregados e solucionar problemas de performance e eventos de limite.

A seguir estão alguns campos importantes na visualização desempenho: Todos os agregados.

- Tipo: O tipo de agregado:



- HDD
  - Híbrida. Combina HDDs e SSDs, mas o Flash Pool não foi ativado.
  - Híbrido (Flash Pool). Combina HDDs e SSDs e o Flash Pool foi ativado.
  - SSD
  - SSD (FabricPool). Combina SSDs e uma camada de nuvem
  - HDD (FabricPool). Combina HDDs e uma camada de nuvem
  - VMDisk (SDS). Discos virtuais dentro de uma máquina virtual
  - VMDisk (FabricPool). Combina discos virtuais e uma camada de nuvem
  - LUN (FlexArray)
- Relatório de dados inativos: Se a capacidade de relatório de dados inativos está ativada ou desativada neste agregado. Quando ativado, os volumes desse agregado exibem a quantidade de dados inativos na exibição desempenho: Todos os volumes. O valor neste campo é "N/A" quando a versão do ONTAP não suporta relatórios de dados inativos.
  - Política de limite: A política de limite de desempenho definido pelo usuário, ou políticas, que estão ativas neste objeto de storage. Você pode posicionar o cursor sobre os nomes de políticas que contêm uma elipse (...) para exibir o nome completo da política ou a lista de nomes de políticas atribuídos. Os botões Assign Performance Threshold Policy e Clear Performance Threshold Policy permanecem desabilitados até que você selecione um ou mais objetos clicando nas caixas de seleção localizadas à esquerda. Consulte os links a seguir para obter mais informações:
    - ["Atribuindo políticas de limite de desempenho a objetos de storage"](#)
    - ["Remoção de políticas de limite de performance de objetos de storage"](#)

### Performance: Visualização de todos os nós

A visualização desempenho: Todos os nós exibe uma visão geral dos eventos de performance, dados e informações de configuração de cada nó que está sendo monitorado por uma instância do Unified Manager. Isso permite que você monitore rapidamente a performance de seus nós e solucione problemas de performance e eventos de limite.



O Flash Cache Reads retorna a porcentagem de operações de leitura no nó que são satisfeitas pelo cache, em vez de serem retornadas do disco. Os dados do Flash Cache são exibidos somente para nós e somente quando um módulo Flash Cache é instalado no nó.

No menu **relatórios**, a opção **Relatório de inventário de hardware** é fornecida quando o Unified Manager e os clusters que ele está gerenciando são instalados em um site sem conectividade de rede externa. Esse botão gera um arquivo .csv que contém uma lista completa de informações de cluster e nó, como números de modelo de hardware e números de série, tipos e contagens de disco, licenças instaladas e muito mais. Essa funcionalidade de relatórios é útil para a renovação de contratos em sites seguros que não estão conectados à plataforma NetApp Active IQ. Você pode atribuir políticas de limite de desempenho ou limpar políticas de limite de qualquer objeto nas páginas de inventário de objetos usando os botões **atribuir política de limite de desempenho** e **Limpar política de limite de desempenho**.

Consulte os links a seguir para obter mais informações:

- ["Atribuindo políticas de limite de desempenho a objetos de storage"](#)
- ["Remoção de políticas de limite de performance de objetos de storage"](#)
- ["Gerando um relatório de inventário de hardware para renovação de contrato"](#)

## Performance: Visualização de todas as VMs de storage

A visualização desempenho: Todas as VMs de storage exibe uma visão geral dos eventos de performance, dados e informações de configuração de cada máquina virtual de storage (SVM) que está sendo monitorada por uma instância do Unified Manager. Isso permite que você monitore rapidamente a performance de seus SVMs e solucione problemas de performance e eventos de limite. O campo latência desta página relata o tempo médio de resposta para todas as solicitações de e/S, expresso em milissegundos por operação.



Os SVMs listados nesta página incluem somente dados e SVMs de cluster. O Unified Manager não usa nem exibe SVMs de Admin ou nó.

Consulte os links a seguir para obter mais informações:

- ["Atribuindo políticas de limite de desempenho a objetos de storage"](#)
- ["Remoção de políticas de limite de performance de objetos de storage"](#)

## Performance: Visualização de todos os LUNs

A visualização desempenho: Todos os LUNs exibe uma visão geral dos eventos de performance, dados e informações de configuração de cada LUN que está sendo monitorado por uma instância do Unified Manager. Isso permite que você monitore rapidamente a performance dos LUNs e solucione problemas de performance e eventos de limite.

Se você quiser analisar a latência e a taxa de transferência de um objeto específico, clique no ícone mais , depois em **analisar carga de trabalho** e você pode visualizar gráficos de desempenho e capacidade na página **análise de carga de trabalho**.

Consulte os links a seguir para obter mais informações:

- ["Monitoramento de LUNs em uma relação de Grupo de consistência"](#)
- ["Provisionamento de LUNs"](#)
- ["Atribuindo políticas de limite de desempenho a objetos de storage"](#)
- ["Remoção de políticas de limite de performance de objetos de storage"](#)
- ["Exibindo volumes ou LUNs que estão no mesmo grupo de políticas de QoS"](#).
- ["Exibindo as configurações do grupo de políticas de QoS aplicadas a volumes ou LUNs específicos"](#)
- ["Provisionamento de LUNs usando APIs"](#)

## Performance: Visualização de todos os namespaces NVMe

A visualização desempenho: Todos os namespaces NVMe exibe uma visão geral dos eventos de performance, dados e informações de configuração de cada namespace NVMe que está sendo monitorado por uma instância do Unified Manager. Isso permite que você monitore rapidamente a performance e a integridade dos namespaces e solucione problemas e eventos de limite.

As seguintes informações, entre outras, são relatadas: O estado atual do namespace. \* Offline - o acesso de leitura ou gravação ao namespace não é permitido. \* Online - o acesso de leitura e gravação ao namespace é permitido. \* NVFail - o namespace foi automaticamente colocado offline devido a uma falha do NVRAM. \* Erro de espaço - o namespace ficou sem espaço.

Consulte os links a seguir para obter mais informações:

- ["Atribuindo políticas de limite de desempenho a objetos de storage"](#)
- ["Remoção de políticas de limite de performance de objetos de storage"](#)

### Desempenho: Visualização de todas as interfaces de rede

A exibição desempenho: Todas as interfaces de rede exibe uma visão geral dos eventos de desempenho, dados e informações de configuração para cada interface de rede (LIF) que está sendo monitorada por essa instância do Unified Manager. Esta página permite que você monitore rapidamente o desempenho de suas interfaces e solucione problemas de desempenho e eventos de limite. A seguir estão alguns campos importantes na exibição desempenho: Todas as interfaces de rede.

- IOPS: As operações de entrada/saída por segundo. O IOPS não é aplicável a LIFs NFS e LIFs CIFS e é exibido como N/A para esses tipos.
- Latência: O tempo médio de resposta para todas as solicitações de e/S, expresso em milissegundos por operação. A latência não é aplicável a LIFs NFS e LIFs CIFS e é exibida como N/A para esses tipos.
- Localização da casa: A localização da casa para a interface, exibida como nome do nó e nome da porta, separada por dois pontos (:). Se a localização for exibida com uma elipse (...), você pode posicionar o cursor sobre o nome da localização para exibir a localização completa.
- Localização atual: O local atual para a interface, exibido como nome do nó e nome da porta, separados por dois pontos (:). Se a localização for exibida com uma elipse (...), você pode posicionar o cursor sobre o nome da localização para exibir a localização completa.
- Função: A função de interface: Dados, cluster, gerenciamento de nós ou Intercluster.



As interfaces listadas nesta página incluem Data LIFs, Cluster LIFs, Node Management LIFs e clusters LIFs. O Unified Manager não usa nem exibe LIFs do sistema.

### Desempenho: Exibição de todas as portas

A exibição desempenho: Todas as portas exibe uma visão geral dos eventos de desempenho, dados e informações de configuração de cada porta que está sendo monitorada por uma instância do Unified Manager. Isso permite que você monitore rapidamente o desempenho de suas portas e solucione problemas de desempenho e eventos de limite. Para uma função de porta, a função de porta de rede é exibida, seja dados ou Cluster. As portas FCP não podem ter uma função e a função é exibida como N/A.



Os valores do contador de desempenho são exibidos apenas para portas físicas. Os valores de contador não são exibidos para VLANs ou grupos de interface.

Consulte os links a seguir para obter mais informações:

- ["Atribuindo políticas de limite de desempenho a objetos de storage"](#)
- ["Remoção de políticas de limite de performance de objetos de storage"](#)

### Desempenho: Exibição de grupos de diretiva QoS

A visualização grupos de políticas de QoS exibe os grupos de políticas de QoS disponíveis nos clusters que o Unified Manager está monitorando. Isso inclui políticas tradicionais de QoS, políticas de QoS adaptáveis e políticas de QoS atribuídas pelo uso de níveis de serviço de performance.

A seguir estão alguns campos importantes na exibição desempenho: Grupos de políticas de QoS.

- Grupo de políticas de QoS: O nome do grupo de políticas de QoS. Para políticas do NetApp Service Level Manager (NSLM) 1,3 que foram importadas para o Unified Manager 9,7 ou posterior, o nome exibido aqui inclui o nome do SVM e outras informações que não estão no nome quando o nível de Serviço de Performance foi definido no NSLM. Por exemplo, o nome "NSLM\_vs6\_Performance\_2\_0" significa que esta é a política de PSL "Performance" definida pelo sistema NSLM criada na SVM "vs6" com uma latência esperada de "2 ms/op".
- SVM: A VM de storage (SVM) a que pertence o grupo de políticas de QoS. Você pode clicar no nome da VM de armazenamento para navegar até a página de detalhes da VM de armazenamento. Observe que esse campo fica em branco se a política de QoS tiver sido criada na VM de storage Admin, pois esse tipo de VM de storage representa o cluster.
- Taxa de transferência mínima: A taxa de transferência mínima, em IOPS, fornecida pelo grupo de políticas. Para políticas adaptáveis, esse é o IOPS mínimo esperado por TB alocado ao volume ou LUN, com base no tamanho alocado do objeto de storage.
- Taxa de transferência máxima: A taxa de transferência, em IOPS e/ou MB/s, que o grupo de políticas não deve exceder. Quando este campo está em branco significa que o máximo definido em ONTAP é infinito. Para políticas adaptáveis, esse é o máximo (pico) de IOPS possível por TB alocado ao volume ou LUN, com base no tamanho alocado do objeto de armazenamento ou no tamanho usado do objeto de armazenamento.
- IOPS mínimo absoluto: Para políticas adaptáveis, esse é o valor mínimo absoluto de IOPS usado como uma substituição quando o IOPS esperado é menor que esse valor.
- Tamanho do bloco: O tamanho do bloco especificado para a política adaptativa de QoS.
- Alocação mínima: Se "espaço alocado" ou "espaço usado" é usado para determinar o throughput máximo (pico) IOPS.
- Latência esperada: A latência média esperada para operações de entrada/saída de storage.
- Compartilhado: Para políticas de QoS tradicionais, se os valores de taxa de transferência definidos no grupo de políticas são compartilhados entre vários objetos.
- Objetos associados: O número de cargas de trabalho atribuídas ao grupo de políticas de QoS. Você pode clicar no botão expandir (▼) ao lado do Nome do Grupo de políticas de QoS para exibir mais detalhes sobre o grupo de políticas.
- Capacidade alocada: A quantidade de espaço que os objetos que estão no grupo de políticas de QoS estão usando atualmente.
- Objetos associados: O número de workloads atribuídos ao grupo de políticas de QoS, separados em volumes e LUNs. Você pode clicar no número para navegar para uma página que forneça mais detalhes sobre os volumes ou LUNs selecionados.

Para obter mais informações, consulte os tópicos em ["Gerenciando o desempenho usando informações de grupo de políticas de QoS"](#).

## Refinando o conteúdo da página de inventário de desempenho

As páginas de inventário para objetos de desempenho contêm ferramentas que ajudam a refinar o conteúdo de dados de inventário de objetos, permitindo localizar dados específicos de forma rápida e fácil.

As informações contidas nas páginas de inventário de objetos Performance podem ser extensas, muitas vezes abrangendo várias páginas. Esse tipo de dados abrangentes é excelente para monitorar, rastrear e melhorar o desempenho; no entanto, localizar dados específicos requer ferramentas para permitir que você localize rapidamente os dados para os quais você está procurando. Portanto, as páginas de inventário de

objetos Performance contêm funcionalidade para pesquisa, classificação e filtragem. Além disso, a pesquisa e a filtragem podem trabalhar em conjunto para restringir ainda mais seus resultados.

## Pesquisar nas páginas desempenho Stock Objeto

Você pode pesquisar strings em páginas de desempenho de inventário de objetos. Use o campo **Search** localizado no canto superior direito da página para localizar rapidamente dados com base no nome do objeto ou no nome da política. Isso permite localizar rapidamente objetos específicos e seus dados associados, ou localizar rapidamente políticas e exibir dados de objeto de política associados.

### Passo

1. Execute uma das seguintes opções, com base nos requisitos de pesquisa:

Para localizar este...	Digite este texto...
Um objeto específico	O nome do objeto no campo <b>Search</b> e clique em <b>Search</b> . O objeto para o qual você pesquisou e seus dados relacionados é exibido.
Uma política de limite de desempenho definido pelo usuário	Todo ou parte do nome da política no campo <b>pesquisar</b> e clique em <b>pesquisar</b> . Os objetos atribuídos à política para a qual você pesquisou são exibidos.

## Classificação nas páginas desempenho do inventário de objetos

Você pode classificar todos os dados em páginas de desempenho de inventário de objetos por qualquer coluna em ordem crescente ou decrescente. Isso permite localizar rapidamente dados de inventário de objetos, o que é útil ao examinar o desempenho ou iniciar um processo de solução de problemas.

A coluna selecionada para classificação é indicada por um nome de cabeçalho de coluna realçado e por um ícone de seta que indica a direção de classificação à direita do nome. Uma seta para cima indica a ordem ascendente; uma seta para baixo indica a ordem descendente. A ordem de classificação padrão é por **Status** (criticidade do evento) em ordem decrescente, com os eventos de desempenho mais críticos listados primeiro.

### Passo

1. Você pode clicar no nome de uma coluna para alternar a ordem de classificação da coluna em ordem ascendente ou descendente.

O conteúdo da página desempenho de inventário de objetos é classificado em ordem crescente ou decrescente, com base na coluna selecionada.

## Filtrando dados nas páginas desempenho do inventário de objetos

Você pode filtrar dados nas páginas desempenho do inventário de objetos para localizar rapidamente dados com base em critérios específicos. Você pode usar a filtragem para restringir o conteúdo das páginas desempenho do inventário de objetos para mostrar

apenas os resultados especificados. Isso fornece um método muito eficiente de exibir apenas os dados de desempenho em que você está interessado.

Você pode usar o painel filtragem para personalizar a exibição de grade com base em suas preferências. As opções de filtro disponíveis são baseadas no tipo de objeto que está sendo visualizado na grade. Se os filtros forem aplicados atualmente, o número de filtros aplicados será exibido à direita do botão filtro.

Três tipos de parâmetros de filtro são suportados.

Parâmetro	Validação
Cadeia de caracteres (texto)	Os operadores são <b>contém, começa com, termina com</b> e <b>não contém</b> .
Número	Os operadores são <b>maiores que, menos que, no último</b> e <b>entre</b> .
Enum (texto)	Os operadores são <b>is</b> e <b>não</b> .

Os campos coluna, Operador e valor são necessários para cada filtro; os filtros disponíveis refletem as colunas filtráveis na página atual. O número máximo de filtros que você pode aplicar é de quatro. Os resultados filtrados são baseados em parâmetros de filtro combinados. Os resultados filtrados aplicam-se a todas as páginas da pesquisa filtrada, não apenas à página exibida atualmente.

Você pode adicionar filtros usando o painel filtragem.

1. Na parte superior da página, clique no botão **filtro**. O painel filtragem é exibido.
2. Clique na lista suspensa esquerda e selecione um objeto; por exemplo, *Cluster* ou um contador de desempenho.
3. Clique na lista pendente central e selecione o operador que pretende utilizar.
4. Na última lista, selecione ou insira um valor para concluir o filtro para esse objeto.
5. Para adicionar outro filtro, clique em \* Adicionar filtro\*. É apresentado um campo de filtro adicional. Conclua este filtro usando o processo descrito nas etapas anteriores. Observe que ao adicionar seu quarto filtro, o botão \* Adicionar filtro \* não é mais exibido.
6. Clique em **Apply Filter** (aplicar filtro). As opções de filtro são aplicadas à grade e o número de filtros é exibido à direita do botão filtro.
7. Use o painel filtragem para remover filtros individuais clicando no ícone de lixeira à direita do filtro a ser removido.
8. Para remover todos os filtros, clique em **Reset** na parte inferior do painel de filtragem.

#### Exemplo de filtragem

A ilustração mostra o painel filtragem com três filtros. O botão \* Adicionar filtro \* é exibido quando você tem menos do que o máximo de quatro filtros.

MBps	greater than	5	MBps	
Node	name starts with	test		
Type	is	FCP Port		
+ Add Filter				
				<input type="button" value="Cancel"/> <input type="button" value="Apply Filter"/>

Depois de clicar em **Apply Filter**, o painel Filtering fecha, aplica os filtros e mostra o número de filtros aplicados ( 3 ).

## Compreensão das recomendações do Unified Manager para categorizar dados na nuvem

A exibição desempenho: Todos os volumes exibe informações relacionadas ao tamanho dos dados do usuário armazenados no volume inativo (frio). Em alguns casos, o Unified Manager identifica certos volumes que se beneficiariam ao separar os dados inativos na camada de nuvem (fornecedor de nuvem ou StorageGRID) de um agregado habilitado para FabricPool.



O FabricPool foi introduzido no ONTAP 9.2. Portanto, se você estiver usando uma versão do software ONTAP anterior a 9,2, a recomendação do Gerenciador Unificado de categorizar dados requer a atualização do software ONTAP. Além disso, a **auto** política de disposição em camadas foi introduzida no ONTAP 9.4 e a **all** política de disposição em camadas foi introduzida no ONTAP 9.6. Portanto, se a recomendação for usar a política de disposição em camadas automática, você precisará atualizar para o ONTAP 9.4 ou superior.

Os três campos a seguir sobre performance: All volumes view fornecem informações sobre se você pode aprimorar a utilização de disco do sistema de storage e economizar espaço na categoria de performance, movendo dados inativos para a camada de nuvem.

- **Política de disposição em camadas**

A política de disposição em categorias determina se os dados no volume permanecem na categoria de performance ou se alguns deles são movidos da categoria de performance para a categoria de nuvem.

O valor neste campo indica a política de disposição em camadas definida no volume, mesmo que o volume não esteja atualmente em um agregado FabricPool. A política de disposição em categorias só entra em vigor quando o volume está em um agregado FabricPool.

- **Dados inativos**

Os dados inativos exibem o tamanho dos dados do usuário armazenados no volume que está inativo (frio).

Um valor é exibido aqui somente quando se usa o software ONTAP 9.4 ou superior porque exige que o agregado no qual o volume é implantado tenha o **inactive data reporting parameter** definido como **enabled** e que o limite de número mínimo de dias de resfriamento tenha sido atendido (para

volumes que usam a **snapshot-only** política de disposição em camadas ou **auto** ). Caso contrário, o valor é listado como "N/A".

#### • **Recomendação de nuvem**

Depois de coletar informações suficientes sobre a atividade de dados no volume, o Unified Manager pode determinar que não há nenhuma ação necessária ou que você pode economizar espaço na categoria de performance ao categorizar dados inativos na camada de nuvem.



O campo dados inativos é atualizado a cada 15 minutos, mas o campo Recomendação da nuvem é atualizado a cada 7 dias quando a análise de dados inativos é realizada no volume. Portanto, a quantidade exata de dados frios pode diferir entre os campos. O campo Recomendação da nuvem exibe a data em que a análise foi executada.

Quando o Relatório de dados inativos está ativado, o campo dados inativos exibe a quantidade exata de dados inativos. Sem a funcionalidade de relatórios de dados inativos o Unified Manager usa estatísticas de performance para determinar se os dados estão inativos em um volume. A quantidade de dados inativos não é exibida no campo dados inativos neste caso, mas é exibida quando você passa o cursor sobre a palavra **Tier** para exibir a recomendação de nuvem.

As recomendações de nuvem que você verá são:

- **Aprendizagem.** Não foram coletados dados suficientes para fazer uma recomendação.
- **Nível.** A análise determinou que o volume contém dados inativos (frios) e que você deve configurar o volume para movê-los para a camada de nuvem. Em alguns casos, isso pode exigir que você mova o volume para um agregado habilitado para FabricPool primeiro. Em outros casos em que o volume já está em um agregado FabricPool, você só precisa alterar a política de disposição em categorias.
- **Nenhuma ação.** Ou o volume tem muito pouco dados inativos, o volume já está definido como a política de disposição em camadas "automática" em um agregado FabricPool ou o volume é um volume de proteção de dados. Esse valor também é exibido quando o volume está off-line ou quando está sendo usado em uma configuração do MetroCluster.

Para mover um volume ou alterar a política de disposição em categorias de volume ou as configurações de relatórios de dados inativos agregados, use o Gerenciador de sistema do ONTAP, os comandos de CLI do ONTAP ou uma combinação dessas ferramentas.

Se você estiver conectado ao Unified Manager com a função Administrador de aplicativos ou Administrador de armazenamento, o link **Configurar volume** estará disponível na recomendação de nuvem quando você passar o cursor sobre a palavra **nível**. Clique neste botão para abrir a página volumes no System Manager para efetuar a alteração recomendada.

## **Monitoramento do desempenho usando as páginas do Performance Explorer**

As páginas do Performance Explorer exibem informações detalhadas sobre o desempenho de cada objeto em um cluster. A página fornece uma visão detalhada do desempenho de todos os objetos de cluster, permitindo que você selecione e compare os dados de desempenho de objetos específicos em vários períodos de tempo.

Você também pode avaliar o desempenho geral de todos os objetos e comparar os dados de desempenho do objeto em um formato lado a lado.



## Entendendo o objeto raiz

O objeto raiz é a linha de base contra a qual outras comparações de objetos são feitas. Isso permite visualizar e comparar os dados de outros objetos com o objeto raiz, fornecendo análise de dados de desempenho que ajuda você a solucionar problemas e melhorar o desempenho dos objetos.

O nome do objeto raiz é exibido na parte superior do painel de comparação. Objetos adicionais são exibidos abaixo do objeto raiz. Embora não haja limite para o número de objetos adicionais que você pode adicionar ao painel de comparação, apenas um objeto raiz é permitido. Os dados para o objeto raiz são exibidos automaticamente nos gráficos no painel Cartas Contadoras.

Você não pode alterar o objeto raiz; ele é sempre definido para a página do objeto que você está visualizando. Por exemplo, se você abrir a página Explorador de desempenho de volume de Volume1, então Volume1 é o objeto raiz e não pode ser alterado. Se você quiser comparar com um objeto raiz diferente, então você deve clicar no link de um objeto e abrir sua página de destino.



Eventos e limites são exibidos apenas para objetos raiz.

## Aplicar filtragem para reduzir a lista de objetos correlacionados na grade

A filtragem permite exibir um subconjunto menor e mais bem definido de objetos na grade. Por exemplo, se você tiver 25 volumes na grade, a filtragem permite exibir somente os volumes que têm taxa de transferência inferior a 90 Mbps ou latência superior a 1 ms/op.

## Especificar um intervalo de tempo para objetos correlacionados

O seletor intervalo de tempo na página Explorador de desempenho permite especificar o intervalo de tempo para a comparação de dados do objeto. Especificar um intervalo de tempo refina o conteúdo das páginas do Performance Explorer para mostrar apenas os dados do objeto dentro do intervalo de tempo especificado.

Refinar o intervalo de tempo fornece um método eficiente de exibir apenas os dados de desempenho em que você está interessado. Pode selecionar um intervalo de tempo predefinido ou especificar um intervalo de tempo personalizado. O intervalo de tempo predefinido é as 72 horas anteriores.

### Selecionar um intervalo de tempo predefinido

Selecionar um intervalo de tempo predefinido é uma forma rápida e eficiente de personalizar e focar a saída de dados ao visualizar dados de desempenho de objetos de cluster. Ao selecionar um intervalo de tempo predefinido, estão disponíveis dados de até 13 meses.

### Passos

1. No canto superior direito da página **Performance Explorer**, clique em **intervalo de tempo**.
2. No lado direito do painel **Time Range Selection** (seleção de intervalo de tempo), selecione um intervalo de tempo predefinido.

3. Clique em **aplicar intervalo**.

### Especificar um intervalo de tempo personalizado

A página Explorador de desempenho permite especificar a data e o intervalo de tempo para os dados de desempenho. Especificar um intervalo de tempo personalizado proporciona maior flexibilidade do que usar intervalos de tempo predefinidos ao refinar dados de objetos de cluster.

Pode selecionar um intervalo de tempo entre uma hora e 390 dias. 13 meses equivale a 390 dias porque cada mês é contado como 30 dias. Especificar um intervalo de data e hora fornece mais detalhes e permite que você amplie eventos de desempenho específicos ou séries de eventos. Especificar um intervalo de tempo também auxilia na solução de problemas potenciais de desempenho, já que especificar um intervalo de data e hora exibe os dados em torno do evento de desempenho em detalhes mais detalhados. Use o controle **intervalo de tempo** para selecionar intervalos de data e hora predefinidos ou especifique seu próprio intervalo de data e hora personalizado de até 390 dias. Os botões para intervalos de tempo predefinidos variam de **Last Hour** a **Last 13 months**.

Selecionar a opção **últimos 13 meses** ou especificar um intervalo de datas personalizado superior a 30 dias exibe uma caixa de diálogo alertando que os dados de desempenho exibidos por um período superior a 30 dias são mapeados usando médias horárias e não polling de dados de 5 minutos. Portanto, uma perda de granularidade visual da linha do tempo pode ocorrer. Se você clicar na opção **não mostrar novamente** na caixa de diálogo, a mensagem não será exibida quando você selecionar a opção **últimos 13 meses** ou especificar um intervalo de datas personalizado maior que 30 dias. Os dados de resumo também se aplicam a um intervalo de tempo menor, se o intervalo de tempo incluir uma hora/data que seja superior a 30 dias a partir de hoje.

Ao selecionar um intervalo de tempo (personalizado ou predefinido), os intervalos de tempo de 30 dias ou menos são baseados em amostras de dados de intervalo de 5 minutos. Intervalos de tempo superiores a 30 dias são baseados em amostras de dados de intervalo de uma hora.

From							To						
April 2015							April 2015						
Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	01	02	03	04	29	30	31	01	02	03	04
05	06	07	08	09	10	11	05	06	07	08	09	10	11
12	13	14	15	16	17	18	12	13	14	15	16	17	18
19	20	21	22	23	24	25	19	20	21	22	23	24	25
26	27	28	29	30	01	02	26	27	28	29	30	01	02
03	04	05	06	07	08	09	03	04	05	06	07	08	09

Time: 6:00 am      Time: 6:00 am

- Last Hour
- Last 24 Hours
- Last 72 Hours
- Last 7 Days
- Last 30 Days
- Last 13 Months
- Custom Range

Cancel      Apply Range

1. Clique na caixa suspensa **intervalo de tempo** e o painel intervalo de tempo será exibido.
2. Para selecionar um intervalo de tempo predefinido, clique num dos botões **Last...** à direita do painel **Time Range**. Ao selecionar um intervalo de tempo predefinido, estão disponíveis dados de até 13 meses. O botão de intervalo de tempo predefinido selecionado é realçado e os dias e horas correspondentes são apresentados nos calendários e seletores de tempo.
3. Para selecionar um intervalo de datas personalizado, clique na data de início no calendário **de** à esquerda.

Clique em \* **ou** \*> para navegar para a frente ou para trás no calendário. Para especificar a data de fim, clique em uma data no calendário **para** à direita. Observe que a data de término padrão é hoje, a menos que você especifique uma data de término diferente. O botão **Custom Range** (intervalo personalizado) à direita do painel Time Range (intervalo de tempo) é realçado, indicando que selecionou um intervalo de datas personalizado.

4. Para selecionar um intervalo de tempo personalizado, clique no controle **hora** abaixo do calendário **de** e selecione a hora de início. Para especificar a hora final, clique no controle **hora** abaixo do calendário **para** à direita e selecione a hora final. O botão **Custom Range** (intervalo personalizado) à direita do painel Time Range (intervalo de tempo) é realçado, indicando que selecionou um intervalo de tempo personalizado.
5. Opcionalmente, você pode especificar os horários de início e término ao selecionar um intervalo de datas predefinido. Selecione o intervalo de datas predefinido conforme descrito anteriormente e, em seguida, selecione as horas de início e de fim, conforme descrito anteriormente. As datas selecionadas são realçadas nos calendários, as horas de início e fim especificadas são exibidas nos controles **hora** e o botão **intervalo personalizado** é realçado.
6. Depois de selecionar o intervalo de data e hora, clique em **aplicar intervalo**. As estatísticas de desempenho para esse intervalo de tempo são exibidas nos gráficos e na linha do tempo de eventos.

## Definir a lista de objetos correlacionados para gráficos de comparação

Você pode definir uma lista de objetos correlacionados para comparação de dados e desempenho no painel Counter Chart. Por exemplo, se a máquina virtual de storage (SVM) tiver algum problema de performance, você poderá comparar todos os volumes no SVM para identificar qual volume pode estar causando o problema.


Você pode adicionar qualquer objeto na grade objetos correlacionados aos painéis comparação e Gráfico de Contador. Isso permite que você visualize e compare dados de vários objetos e com o objeto raiz. Você pode adicionar e remover objetos de e para a grade de objetos correlacionados; no entanto, o objeto raiz no painel de comparação não é removível.




Adicionar muitos objetos ao painel de comparação pode ter um impacto negativo no desempenho. Para manter o desempenho, você deve selecionar um número limitado de gráficos para comparação de dados.

### Passos

1. Na grade objetos, localize o objeto que você deseja adicionar e clique no botão **Adicionar**.

O botão **Add** fica cinza e o objeto é adicionado à lista de objetos adicionais no painel de comparação. Os dados do objeto são adicionados aos gráficos nos painéis gráficos do contador. A cor do ícone de olho do objeto (  ) corresponde à cor da linha de tendência de dados do objeto nos gráficos.

2. **Opcional:** Ocultar ou mostrar dados para objetos selecionados:

Para fazer isso...	Tome esta ação...
Ocultar um objeto selecionado	Clique no ícone olho do objeto selecionado (  ) no painel de comparação. Os dados do objeto ficam ocultos e o ícone de olho desse objeto fica cinza.

Para fazer isso...	Tome esta ação...
Mostrar um objeto oculto	<p>Clique no ícone de olho cinzento do objeto selecionado no painel de comparação.</p> <p>O ícone de olho retorna à sua cor original e os dados do objeto são adicionados de volta aos gráficos no painel Cartas Contadoras.</p>

### 3. Opcional: Remover objetos selecionados do painel **comparando**:

Para fazer isso...	Tome esta ação...
Remover um objeto selecionado	<p>Passe o Mouse sobre o nome do objeto selecionado no painel comparação para mostrar o botão remover objeto (X) e clique no botão. O objeto é removido do painel de comparação e seus dados são limpos dos gráficos de contador.</p>
Remova todos os objetos selecionados	<p>Clique no botão remover todos os objetos (X) na parte superior do painel de comparação. Todos os objetos selecionados e seus dados são removidos, deixando apenas o objeto raiz.</p>

## Compreender as tabelas de contadores

Os gráficos no painel gráficos de contador permitem visualizar e comparar dados de desempenho para o objeto raiz e para os objetos que você adicionou da grade de objetos correlacionados. Isso pode ajudá-lo a entender as tendências de desempenho e isolar e resolver problemas de desempenho.

Os gráficos de contador exibidos por padrão são Eventos, latência, IOPS e Mbps. Os gráficos opcionais que você pode optar por exibir são utilização, capacidade de desempenho usada, IOPS disponíveis, IOPS/TB e taxa de perda de cache. Além disso, você pode optar por exibir valores totais ou valores de divisão para os gráficos de latência, IOPS, Mbps e capacidade de desempenho usada.

O Performance Explorer exibe determinados gráficos de contador por padrão, independentemente de o objeto de armazenamento suportar todos eles ou não. Quando um contador não é suportado, o contador está vazio e a mensagem `Not applicable for <object>` é apresentada.

Os gráficos exibem tendências de desempenho para o objeto raiz e para todos os objetos selecionados no painel comparação. Os dados em cada gráfico são organizados da seguinte forma:

- **Eixo X**

Apresenta o período de tempo especificado. Se você não tiver especificado um intervalo de tempo, o padrão será o período de 72 horas anterior.

- **Eixo Y**

Exibe unidades de contador exclusivas para o objeto selecionado, ou objetos.

As cores da linha de tendência correspondem à cor do nome do objeto, conforme exibido no painel de comparação. Você pode posicionar o cursor sobre um ponto em qualquer linha de tendência para visualizar detalhes de tempo e valor para esse ponto.

Se você quiser investigar um período específico de tempo dentro de um gráfico, você pode usar um dos seguintes métodos:

- Use o botão \* para expandir o painel gráficos de contador para estender a largura da página.
- Use o cursor (quando ele faz a transição para uma lupa) para selecionar uma parte do período de tempo no gráfico para focar e ampliar essa área. Você pode clicar em Redefinir Zoom de Gráfico para retornar o gráfico ao período de tempo padrão.
- Use o botão **Zoom View** para exibir um gráfico de contador único grande que contém detalhes expandidos e indicadores de limite.



Ocasionalmente, as lacunas nas linhas de tendência são exibidas. As lacunas significam que o Unified Manager não conseguiu coletar dados de desempenho do sistema de storage ou que o Unified Manager pode estar inativo.

## Tipos de gráficos de contador de desempenho

Existem gráficos de desempenho padrão que exibem os valores do contador para o objeto de armazenamento selecionado. Cada um dos gráficos do contador de avarias exibe os valores totais separados em ler, escrever e outras categorias. Além disso, alguns gráficos de contador de avarias apresentam detalhes adicionais quando o gráfico é apresentado na vista Zoom.

A tabela a seguir mostra os gráficos de contador de desempenho disponíveis.

Gráficos disponíveis	Descrição da carta
Eventos	Exibe eventos críticos, erros, avisos e informações em correlação com os gráficos estatísticos para o objeto raiz. Os eventos de saúde são exibidos além dos eventos de desempenho para fornecer uma visão completa dos motivos pelos quais o desempenho pode ser afetado.
Latência - total	Número de milissegundos necessários para responder às solicitações do aplicativo. Observe que os valores médios de latência são ponderados por e/S.
Latência - avaria	As mesmas informações mostradas no total da latência, mas com os dados de desempenho separados em leitura, gravação e outra latência. Essa opção de gráfico se aplica somente quando o objeto selecionado é SVM, nó, agregado, volume, LUN ou namespace.

Gráficos disponíveis	Descrição da carta
Latência - componentes do cluster	As mesmas informações mostradas no total da latência, mas com os dados de desempenho separados em latência por componente do cluster. Esta opção de gráfico aplica-se apenas quando o objeto selecionado é um volume.
IOPS - total	Número de operações de entrada/saída processadas por segundo. Quando exibido para um nó, selecionar "Total" exibe o IOPS para dados que se movem através desse nó que podem residir no nó local ou remoto e selecionar "Total (local)" exibe o IOPS para dados que residem apenas no nó atual.
IOPS - avaria	<p>As mesmas informações mostradas no total de IOPS, mas com os dados de performance separados em leitura, gravação e outros IOPS. Essa opção de gráfico se aplica somente quando o objeto selecionado é SVM, nó, agregado, volume, LUN ou namespace.</p> <p>Quando exibido na visualização Zoom, o gráfico de volumes exibe os valores de throughput mínimo e máximo de QoS, se configurado no ONTAP.</p> <p>Quando exibido para um nó, selecionar "Breakdown" exibe a divisão de IOPS para dados que se movem através deste nó que podem residir no nó local ou remoto e selecionar "Breakdown (local)" exibe a divisão de IOPS para dados que residem apenas no nó atual.</p>
IOPS - Protocolos	As mesmas informações mostradas no total de IOPS, mas os dados de performance são separados em gráficos individuais para tráfego de protocolos CIFS, NFS, FCP, NVMe e iSCSI. Essa opção de gráfico se aplica somente quando o objeto selecionado é um SVM.

Gráficos disponíveis	Descrição da carta
IOPS/TB - total	<p>Número de operações de entrada/saída processadas por segundo com base no espaço total que está sendo consumido pela carga de trabalho, em terabytes. Também chamado de densidade de e/S, este contador mede quanto desempenho pode ser entregue por uma determinada quantidade de capacidade de armazenamento. Quando exibido na visualização Zoom, o gráfico de volumes exibe os valores de taxa de transferência esperada e de pico de QoS, se configurado no ONTAP.</p> <p>Esta opção de gráfico aplica-se apenas quando o objeto selecionado é um volume.</p>
MB/s - Total	<p>Número de megabytes de dados transferidos de e para o objeto por segundo.</p>
MB/s - avaria	<p>As mesmas informações mostradas no gráfico MB/s, mas com os dados de taxa de transferência separados em leituras de disco, o Flash Cache lê, grava e outros. Quando exibido na visualização Zoom, o gráfico de volumes exibe os valores máximos de taxa de transferência de QoS, se configurado no ONTAP.</p> <p>Essa opção de gráfico se aplica somente quando o objeto selecionado é SVM, nó, agregado, volume, LUN ou namespace.</p> <div data-bbox="846 1220 902 1276" style="border: 1px solid gray; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> <span style="font-size: 18px; font-weight: bold; color: blue;">i</span> </div> <p style="margin-left: 20px;">Os dados do Flash Cache são exibidos somente para nós e somente quando um módulo Flash Cache é instalado no nó.</p>
Capacidade de desempenho utilizada - total	<p>Porcentagem da capacidade de performance consumida pelo nó ou pelo agregado.</p>
Capacidade de desempenho utilizada - avaria	<p>Capacidade de performance dados usados separados em protocolos de usuário e processos de fundo do sistema. Além disso, a quantidade de capacidade de desempenho livre é mostrada.</p>
IOPS disponíveis - total	<p>Número de operações de entrada/saída por segundo que estão atualmente disponíveis (livres) neste objeto. Esse número é o resultado da subtração do IOPS usado atualmente do total de IOPS que o Unified Manager calcula que o objeto pode executar. Esta opção de gráfico aplica-se apenas quando o objeto selecionado é um nó ou agregado.</p>

Gráficos disponíveis	Descrição da carta
Utilização - Total	Porcentagem de recurso disponível do objeto que está sendo usado. A utilização indica a utilização de nós para nós, a utilização de disco para agregados e a utilização de largura de banda para portas. Essa opção de gráfico se aplica somente quando o objeto selecionado é um nó, agregado ou porta.
Taxa de perda de cache - total	Porcentagem de solicitações de leitura de aplicativos clientes que são retornadas do disco em vez de serem retornadas do cache. Esta opção de gráfico aplica-se apenas quando o objeto selecionado é um volume.

## Selecionar gráficos de desempenho a apresentar

A lista suspensa Choose charts (escolher gráficos) permite selecionar os tipos de gráficos de contador de desempenho a serem exibidos no painel Counter Charts (gráficos de contador). Isso permite que você visualize dados e contadores específicos, com base em seus requisitos de desempenho.

### Passos

1. No painel **Counter Charts**, clique na lista suspensa **Choose Charts**.
2. Adicionar ou remover gráficos:

Para...	Faça isso...
Adicionar ou remover gráficos individuais	Clique nas caixas de seleção ao lado dos gráficos que deseja exibir ou ocultar
Adicione todos os gráficos	Clique em <b>Selecionar tudo</b>
Remova todos os gráficos	Clique em <b>Unselect All</b>

Suas seleções de gráfico são exibidas no painel Cartas Contadoras. Observe que, à medida que você adiciona gráficos, os novos gráficos são inseridos no painel gráficos de contador para corresponder à ordem dos gráficos listados na lista suspensa escolher gráficos. A seleção de gráficos adicionais pode exigir rolagem adicional.

## Expandir o painel Cartas de contagem

Você pode expandir o painel gráficos de contador para que os gráficos sejam maiores e mais legíveis.

Depois de definir os objetos de comparação e o intervalo de tempo para contadores, você pode exibir um painel de gráficos de contador maior. Você usa o botão \* no meio da janela do Performance Explorer para expandir o painel.



## Passo

1. Expanda ou reduza o painel **Counter Charts**.

Para...	Faça isso...
Expanda o painel gráficos de contador para ajustar a largura da página	Clique no botão *
Reduza o painel gráficos de contador para a metade direita da página	Clique no botão >

## Alterar a focagem dos gráficos de contador para um período de tempo mais curto

Pode utilizar o rato para reduzir o intervalo de tempo para focar num determinado período de tempo no painel Counter Chart ou na janela Counter Charts Zoom View (visualização de zoom de gráficos de contador). Isso permite que você veja uma visão mais granular e microscópica de qualquer parte do cronograma de dados, eventos e limites de desempenho.

### Antes de começar

O cursor deve ter mudado para uma lupa para indicar que esta funcionalidade está ativa.



Ao usar esse recurso, que altera a linha do tempo para exibir valores que correspondem à exibição mais granular, o intervalo de hora e data no seletor **intervalo de tempo** não muda dos valores originais do gráfico.

### Passos

1. Para aumentar o zoom num determinado período de tempo, clique em utilizar a lupa e arraste o rato para realçar a área que pretende ver em detalhe.

Os valores do contador para o período de tempo selecionado preenchem o gráfico do contador.

2. Para retornar ao período de tempo original, conforme definido no seletor **intervalo de tempo**, clique no botão **Redefinir Zoom do gráfico**.

O contador é apresentado no seu estado original.

## Exibindo detalhes do evento na linha do tempo de Eventos

Você pode exibir todos os eventos e seus detalhes relacionados no painel linha do tempo de Eventos do Performance Explorer. Este é um método rápido e eficiente de visualizar todos os eventos de integridade e desempenho que ocorreram no objeto raiz durante um intervalo de tempo especificado, o que pode ser útil para solucionar problemas de desempenho.

O painel Calendário de Eventos mostra eventos críticos, de erro, de aviso e informativos que ocorreram no objeto raiz durante o intervalo de tempo selecionado. Cada gravidade de evento tem sua própria linha do tempo. Eventos únicos e múltiplos são representados por um ponto de evento na linha do tempo. Você pode posicionar o cursor sobre um ponto de evento para ver os detalhes do evento. Para aumentar a granularidade

visual de vários eventos, você pode diminuir o intervalo de tempo. Isso espalha vários eventos em eventos únicos, permitindo que você visualize e investigue separadamente cada evento.


Cada ponto de evento de desempenho na linha do tempo de Eventos alinha verticalmente com um pico correspondente nas linhas de tendência dos gráficos de contador que são exibidas abaixo da linha do tempo de Eventos. Isso fornece uma correlação visual direta entre eventos e desempenho geral. Eventos de saúde também são exibidos na linha do tempo, mas esses tipos de eventos não necessariamente se alinham com um pico em um dos gráficos de desempenho.

### Passos

1. No painel **cronograma de eventos**, posicione o cursor sobre um ponto de evento em uma linha do tempo para exibir um resumo do evento ou eventos nesse ponto de evento.

Uma caixa de diálogo pop-up exibe informações sobre os tipos de eventos, a data e a hora em que os eventos ocorreram, o estado e a duração do evento.

2. Veja os detalhes completos do evento para um evento ou vários eventos:

Para fazer isso...	Clique aqui...
Exibir detalhes de um único evento	<b>Exibir detalhes do evento</b> na caixa de diálogo pop-up.
Ver detalhes de vários eventos	<b>Exibir Detalhes do evento</b> na caixa de diálogo pop-up.   Clicar em um único evento na caixa de diálogo vários eventos exibe a página Detalhes do evento apropriada.

## Contador gráficos Zoom View

Os gráficos de contador fornecem uma visualização de zoom que permite aumentar o zoom nos detalhes de desempenho durante o período de tempo especificado. Isso permite que você veja detalhes e eventos de desempenho com granularidade muito maior, o que é benéfico para solucionar problemas de desempenho.

Quando exibido na Exibição de Zoom, alguns dos gráficos de detalhamento fornecem informações adicionais do que aparece quando o gráfico não está na Exibição de Zoom. Por exemplo, as páginas de visualização de zoom do gráfico de IOPS, IOPS/TB e Mbps exibem valores de política de QoS para volumes e LUNs se tiverem sido definidos no ONTAP.



Para políticas de limite de desempenho definidas pelo sistema, apenas as políticas "recursos do nó sobreutilizados" e "limite de taxa de transferência de QoS violado" estão disponíveis na lista **políticas**. As outras políticas de limite definidas pelo sistema não estão disponíveis no momento.

## Apresentar a vista de zoom das cartas do contador

A visualização de zoom de gráficos de contador fornece um nível mais fino de detalhes para o gráfico de contador selecionado e sua linha do tempo associada. Isso amplia os dados do gráfico de contador, permitindo que você tenha uma visão mais nítida dos eventos de desempenho e suas causas subjacentes.

Pode apresentar a vista de zoom das cartas de contador para qualquer carta de contador.

### Passos

1. Clique em **Zoom View** para abrir o gráfico selecionado uma nova janela do navegador.
2. Se você estiver exibindo um gráfico de divisão e, em seguida, clique em **Zoom View**, o gráfico de divisão é mostrado em Zoom View. Você pode selecionar **Total** enquanto estiver em Zoom View se quiser alterar a opção de exibição.

## Especificar o intervalo de tempo na Vista Zoom

O controle **intervalo de tempo** na janela Exibição de zoom de gráficos de contador permite especificar um intervalo de data e hora para o gráfico selecionado. Isso permite localizar rapidamente dados específicos com base em um intervalo de tempo predefinido ou em seu próprio intervalo de tempo personalizado.

Pode selecionar um intervalo de tempo entre uma hora e 390 dias. 13 meses equivale a 390 dias porque cada mês é contado como 30 dias. Especificar um intervalo de data e hora fornece mais detalhes e permite que você amplie eventos de desempenho específicos ou séries de eventos. Especificar um intervalo de tempo também auxilia na solução de problemas potenciais de desempenho, já que especificar um intervalo de data e hora exibe os dados em torno do evento de desempenho em detalhes mais detalhados. Use o controle **intervalo de tempo** para selecionar intervalos de data e hora predefinidos ou especifique seu próprio intervalo de data e hora personalizado de até 390 dias. Os botões para intervalos de tempo predefinidos variam de **Last Hour** a **Last 13 months**.

Selecionar a opção **últimos 13 meses** ou especificar um intervalo de datas personalizado superior a 30 dias exibe uma caixa de diálogo alertando que os dados de desempenho exibidos por um período superior a 30 dias são mapeados usando médias horárias e não polling de dados de 5 minutos. Portanto, uma perda de granularidade visual da linha do tempo pode ocorrer. Se você clicar na opção **não mostrar novamente** na caixa de diálogo, a mensagem não será exibida quando você selecionar a opção **últimos 13 meses** ou especificar um intervalo de datas personalizado maior que 30 dias. Os dados de resumo também se aplicam a um intervalo de tempo menor, se o intervalo de tempo incluir uma hora/data que seja superior a 30 dias a partir de hoje.

Ao selecionar um intervalo de tempo (personalizado ou predefinido), os intervalos de tempo de 30 dias ou menos são baseados em amostras de dados de intervalo de 5 minutos. Intervalos de tempo superiores a 30 dias são baseados em amostras de dados de intervalo de uma hora.

1. Clique na caixa suspensa **intervalo de tempo** e o painel intervalo de tempo será exibido.
2. Para selecionar um intervalo de tempo predefinido, clique num dos botões **Last...** à direita do painel **Time Range**. Ao selecionar um intervalo de tempo predefinido, estão disponíveis dados de até 13 meses. O botão de intervalo de tempo predefinido selecionado é realçado e os dias e horas correspondentes são apresentados nos calendários e seletores de tempo.
3. Para selecionar um intervalo de datas personalizado, clique na data de início no calendário **de** à esquerda. Clique em **\* ou \*>** para navegar para a frente ou para trás no calendário. Para especificar a data de fim, clique em uma data no calendário **para** à direita. Observe que a data de término padrão é hoje, a menos que você especifique uma data de término diferente. O botão **Custom Range** (intervalo personalizado) à direita do painel Time Range (intervalo de tempo) é realçado, indicando que selecionou um intervalo de datas personalizado.
4. Para selecionar um intervalo de tempo personalizado, clique no controle **hora** abaixo do calendário **de** e selecione a hora de início. Para especificar a hora final, clique no controle **hora** abaixo do calendário **para** à direita e selecione a hora final. O botão **Custom Range** (intervalo personalizado) à direita do painel Time Range (intervalo de tempo) é realçado, indicando que selecionou um intervalo de tempo personalizado.
5. Opcionalmente, você pode especificar os horários de início e término ao selecionar um intervalo de datas predefinido. Selecione o intervalo de datas predefinido conforme descrito anteriormente e, em seguida, selecione as horas de início e de fim, conforme descrito anteriormente. As datas selecionadas são realçadas nos calendários, as horas de início e fim especificadas são exibidas nos controles **hora** e o botão **intervalo personalizado** é realçado.
6. Depois de selecionar o intervalo de data e hora, clique em **aplicar intervalo**. As estatísticas de desempenho para esse intervalo de tempo são exibidas nos gráficos e na linha do tempo de eventos.

### Selecionar limites de desempenho na visualização de zoom de gráficos de contador

A aplicação de limites na Exibição de Zoom de gráficos de Contador fornece uma visualização detalhada das ocorrências de eventos de limite de desempenho. Isso permite que você aplique ou remova limites e visualize imediatamente os resultados, o que pode ser útil ao decidir se a solução de problemas deve ser sua próxima etapa.

A seleção de limites na Exibição de zoom de gráficos de contador permite visualizar dados precisos sobre eventos de limite de desempenho. Você pode aplicar qualquer limite exibido na área **políticas** da Exibição de Zoom de gráficos de Contador.

Apenas uma política de cada vez pode ser aplicada ao objeto na Exibição de Zoom de gráficos de Contador.

## Passo

1. Selecione ou desmarque a  que está associada a uma política.

O limite selecionado é aplicado à vista de zoom de gráficos de contador. Os limites críticos são exibidos como uma linha vermelha; os limites de aviso são exibidos como uma linha amarela.

## Visualização da latência do volume por componente do cluster

Você pode exibir informações detalhadas de latência de um volume usando a página Explorador de desempenho de volume. O gráfico de latência - contador total mostra a latência total no volume e o gráfico de contagem de latência - discriminação é útil para determinar o impactos da latência de leitura e gravação no volume.

Além disso, o gráfico latência - componentes de cluster mostra uma comparação detalhada da latência de cada componente do cluster para ajudar a determinar como cada componente contribui para a latência total no volume. Os seguintes componentes do cluster são exibidos:


- Rede
- Limite máximo de QoS
- Mín. Limite QoS
- Processamento de rede
- Interconexão de clusters
- Data Processing
- Operações agregadas
- Ativação do volume
- Recursos do MetroCluster
- Latência da nuvem
- Sincronizar SnapMirror

## Passos

1. Na página **volume Performance Explorer** do volume selecionado, no gráfico de latência, selecione **Cluster Components** no menu suspenso.

O gráfico latência - componentes do cluster é exibido.

2. Para exibir uma versão maior do gráfico, selecione **Zoom View**.

É apresentado o gráfico comparativo dos componentes do grupo de instrumentos. Você pode restringir a comparação desmarcando ou selecionando o  que está associado a cada componente do cluster.

3. Para visualizar os valores específicos, mova o cursor para a área do gráfico para ver a janela pop-up.

## Visualização do tráfego de IOPS do SVM por protocolo

Use a página Performance/SVM Explorer para ver informações detalhadas de IOPS de um SVM. O gráfico de IOPS - contador total mostra o uso total de IOPS no SVM, e o gráfico de contador de falhas IOPS - é útil para determinar o impacto de leitura, gravação

e outros IOPS no SVM.

Além disso, o gráfico IOPS - Protocolos mostra uma comparação detalhada do tráfego IOPS para cada protocolo que está sendo usado no SVM. Estão disponíveis os seguintes protocolos:


- CIFS
- NFS
- FCP
- ISCSI
- NVMe-FC

### Passos

1. Na página **Performance/SVM Explorer** do SVM selecionado, no gráfico IOPS, selecione **Protocolos** no menu suspenso.

É apresentado o gráfico IOPS - Protocolos.

2. Para exibir uma versão maior do gráfico, selecione **Zoom View**.

É apresentado o gráfico comparativo do protocolo avançado de IOPS. Pode restringir a comparação desmarcando ou selecionando o  que está associado a um protocolo.

3. Para visualizar os valores específicos, mova o cursor para a área de gráfico de qualquer gráfico para ver a janela pop-up.

## Visualização de gráficos de latência de volume e LUN para verificar a garantia de desempenho

Você pode ver os volumes e LUNs que você assinou no programa "Garantia de desempenho" para verificar se a latência não excedeu o nível que você foi garantido.

A garantia de desempenho de latência é de um milissegundo por valor de operação que não deve ser excedido. Ele é baseado em uma média horária, não no período padrão de coleta de desempenho de cinco minutos.

### Passos

1. Na visualização **desempenho: Todos os volumes** ou **desempenho: Todos os LUNs**, selecione o volume ou LUN em que você está interessado.
2. Na página **Explorador de desempenho** para o volume ou LUN selecionado, escolha **média horária** no seletor **Ver estatísticas em**.

A linha horizontal no gráfico de latência mostrará uma linha mais suave à medida que as coleções de cinco minutos são substituídas pela média horária.

3. Se você tiver outros volumes no mesmo agregado que estão sob a garantia de desempenho, poderá adicionar esses volumes para visualizar o valor de latência no mesmo gráfico.

## Visualização do desempenho de todos os clusters do SAN Array

Você pode usar a visualização desempenho: Todos os clusters para exibir o status de desempenho dos clusters All SAN Array.

## Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Você pode exibir informações gerais de todos os clusters de storage SAN na exibição desempenho: Todos os clusters e detalhes na página Cluster / Performance Explorer.

## Passos

1. No painel de navegação esquerdo, clique em **Storage > clusters**.
2. Certifique-se de que a coluna "personalidade" seja exibida na visualização **Saúde: Todos os clusters** ou adicione-a usando o controle **Mostrar / Ocultar**.

Essa coluna exibe "All SAN Array" para os clusters All SAN Array.

3. Para exibir informações sobre o desempenho nesses clusters, selecione a exibição **desempenho: Todos os clusters**.

Veja as informações de desempenho do cluster All SAN Array.

4. Para exibir informações detalhadas sobre o desempenho nesses clusters, clique no nome de um cluster All SAN Array.
5. Clique na guia **Explorer**.
6. Na página **Cluster / Performance Explorer**, selecione **nós neste Cluster** no menu **Exibir e comparar**.

Você pode comparar as estatísticas de desempenho de ambos os nós nesse cluster para garantir que a carga seja quase idêntica em ambos os nós. Se houver grandes discrepâncias entre os dois nós, você pode adicionar o segundo nó aos gráficos e comparar os valores em um período de tempo mais longo para identificar quaisquer problemas de configuração.

## Visualização de IOPS do nó com base em workloads que residem somente no nó local

O gráfico de contador de IOPS do nó pode destacar onde as operações estão passando somente pelo nó local usando um LIF de rede para executar operações de leitura/gravação em volumes em um nó remoto. Os gráficos de IOPS - total (local)" e "divisão (local)" exibem o IOPS para dados que residem em volumes locais apenas no nó atual.

As versões "locais" desses gráficos de contador são semelhantes aos gráficos de nós para capacidade de desempenho e utilização, pois também mostram apenas as estatísticas de dados que residem em volumes locais.

Ao comparar as versões "locais" desses gráficos de contador com as versões totais regulares desses gráficos de contador, você pode ver se há muito tráfego se movendo através do nó local para acessar volumes no nó remoto. Essa situação pode causar problemas de desempenho, possivelmente indicados pela alta utilização no nó, se houver muitas operações passando pelo nó local para alcançar um volume em um nó remoto. Nesses casos, você pode querer mover um volume para o nó local ou criar um LIF no nó remoto onde o tráfego de hosts que acessam esse volume pode ser conetado.

## Passos

1. Na página **Performance/Node Explorer** do nó selecionado, no gráfico IOPS, selecione **Total** no menu suspenso.

O gráfico IOPS - Total é exibido.

2. Clique em **Zoom View** para exibir uma versão maior do gráfico em uma nova guia do navegador.
3. De volta à página **Performance/Node Explorer**, no gráfico IOPS, selecione **Total (local)** no menu suspenso.

O gráfico IOPS - Total (local) é exibido.

4. Clique em **Zoom View** para exibir uma versão maior do gráfico em uma nova guia do navegador.
5. Visualize ambos os gráficos ao lado uns dos outros e identifique áreas onde os valores de IOPS parecem ser bastante diferentes.
6. Mova o cursor sobre essas áreas para comparar as IOPS local e total de um ponto específico no tempo.

## Componentes das páginas de destino do objeto

As páginas de destino do objeto fornecem detalhes sobre todos os eventos críticos, de aviso e informativos. Eles fornecem uma visão detalhada do desempenho de todos os objetos de cluster, permitindo que você selecione e compare objetos individuais em vários períodos de tempo.

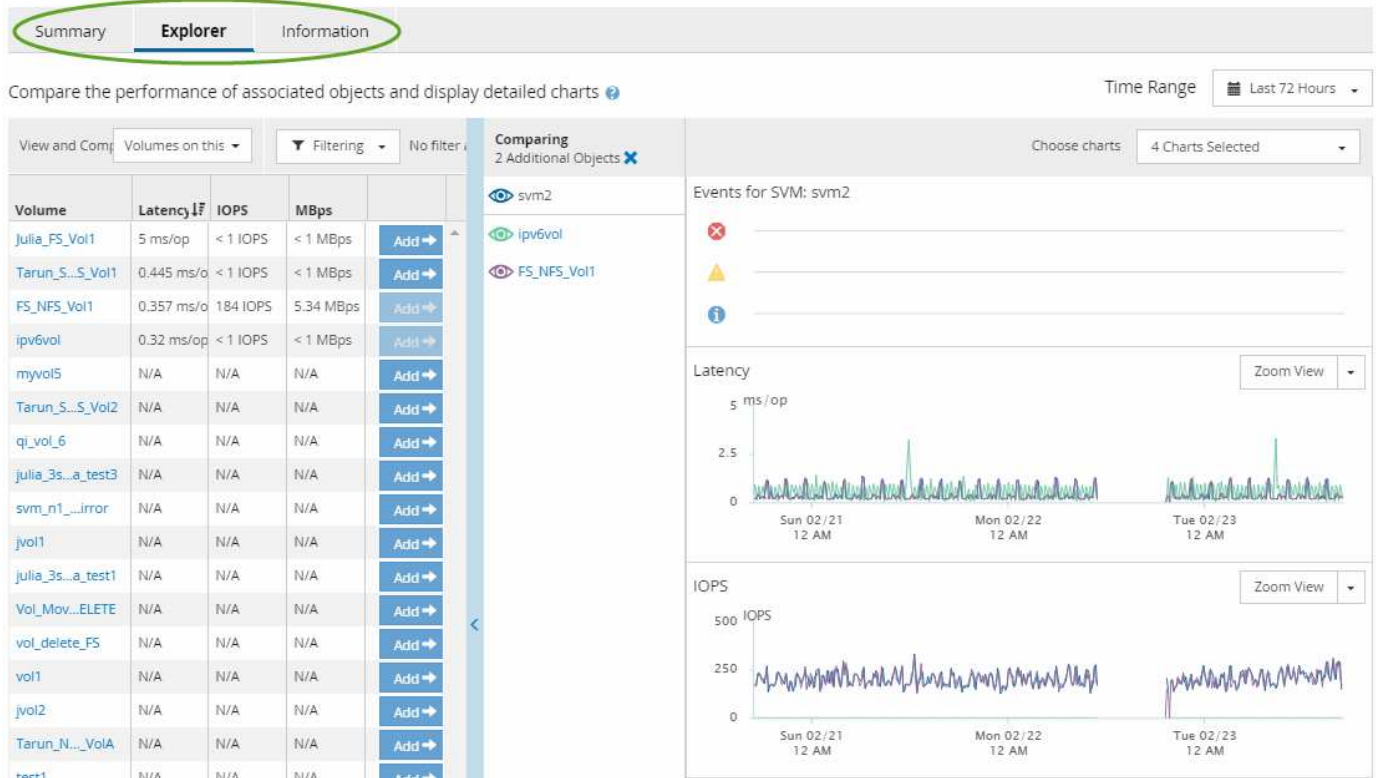
As páginas de destino do objeto permitem examinar o desempenho geral de todos os objetos e comparar os dados de desempenho do objeto em um formato lado a lado. Isso é benéfico ao avaliar o desempenho e ao solucionar problemas de eventos.



Os dados apresentados nos painéis de resumo do contador e nos gráficos do contador baseiam-se num intervalo de amostragem de cinco minutos. Os dados exibidos na grade de inventário de objetos no lado esquerdo da página são baseados em um intervalo de amostragem de uma hora.

A imagem a seguir mostra um exemplo de uma página de destino de objeto que exibe as informações do Explorer:





Dependendo do objeto de armazenamento que está sendo visualizado, a página de destino do objeto pode ter as seguintes guias que fornecem dados de desempenho sobre o objeto:

- **Resumo**

Exibe três ou quatro gráficos de contador contendo os eventos e o desempenho por objeto para o período de 72 horas anterior, incluindo uma linha de tendência que mostra os valores alto e baixo durante esse período.

- **Explorador**

Exibe uma grade de objetos de armazenamento relacionados ao objeto atual, o que permite comparar os valores de desempenho do objeto atual com os dos objetos relacionados. Este separador inclui até onze gráficos de contador e um seletor de intervalo de tempo, que lhe permitem efetuar uma variedade de comparações.

- **Informações**

Exibe valores para atributos de configuração que não são de performance sobre o objeto de storage, incluindo a versão instalada do software ONTAP, o nome do parceiro de HA e o número de portas e LIFs.

- **Top performers**

Para clusters: Exibe os objetos de armazenamento que têm o desempenho mais alto ou o desempenho mais baixo, com base no contador de desempenho selecionado.

- **Planejamento de failover**

Para nós: Exibe a estimativa do impacto na performance em um nó se o parceiro de HA do nó falhar.

- **Detalhes**

Para volumes: Exibe estatísticas detalhadas de desempenho para todas as atividades de e/S e operações para o workload de volume selecionado. Esta guia está disponível para volumes FlexVol, volumes FlexGroup e componentes de FlexGroups.

## **Página de resumo**

A página Resumo exibe gráficos de contador que contêm detalhes sobre os eventos e o desempenho por objeto para o período de 72 horas anterior. Esses dados não são atualizados automaticamente, mas são atualizados a partir do último carregamento da página. Os gráficos na página Resumo respondem à pergunta *preciso procurar mais?*

### **Gráficos e estatísticas de contador**

Os gráficos de resumo fornecem uma visão geral rápida e de alto nível para o último período de 72 horas e ajudam você a identificar possíveis problemas que exigem mais investigação.

As estatísticas do contador de páginas de resumo são apresentadas em gráficos.

Você pode posicionar o cursor sobre a linha de tendência em um gráfico para visualizar os valores do contador para um determinado ponto no tempo. Os gráficos de resumo também exibem o número total de eventos críticos e de aviso ativos para o período de 72 horas anterior para os seguintes contadores:

- **Latência**

Tempo médio de resposta para todas as solicitações de e/S; expresso em milissegundos por operação.

Exibido para todos os tipos de objeto.

- **IOPS**

Velocidade de operação média; expressa em operações de entrada/saída por segundo.

Exibido para todos os tipos de objeto.

- **MB/s**

Taxa de transferência média; expressa em megabytes por segundo.

Exibido para todos os tipos de objeto.

- **Capacidade de desempenho utilizada**

Porcentagem de capacidade de performance consumida por nó ou agregado.

Exibido apenas para nós e agregados.

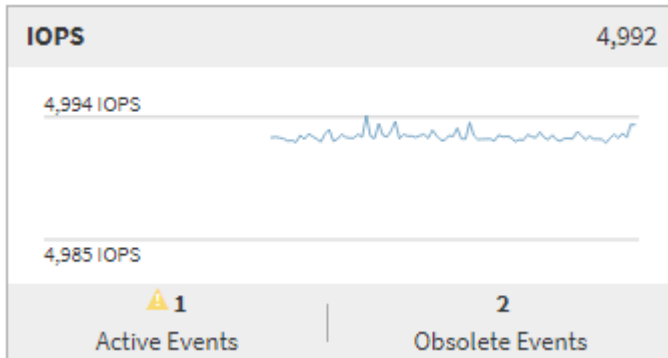
- **Utilização**

Porcentagem de utilização de objetos para nós e agregados ou utilização de largura de banda para portas.

Exibido apenas para nós, agregados e portas.

Posicionar o cursor sobre a contagem de eventos para eventos ativos mostra o tipo e o número de eventos. Os eventos críticos são exibidos em vermelho (■) e os eventos de aviso são exibidos em amarelo (■).

O número no canto superior direito do gráfico na barra cinza é o valor médio do último período de 72 horas. Os números mostrados na parte inferior e superior do gráfico de linhas de tendência são os valores mínimo e máximo para o último período de 72 horas. A barra cinza abaixo do gráfico contém a contagem de eventos ativos (novos e reconhecidos) e eventos obsoletos do último período de 72 horas.



#### • Tabela de contador de latência

O gráfico de contador de latência fornece uma visão geral de alto nível da latência do objeto para o período de 72 horas anterior. Latência refere-se ao tempo médio de resposta para todas as solicitações de e/S; expresso em milissegundos por operação, tempo de serviço, tempo de espera ou ambos experimentados por um pacote de dados ou bloco no componente de armazenamento de cluster em consideração.

**Superior (valor do contador):** o número no cabeçalho exibe a média do período de 72 horas anterior.

**Médio (gráfico de desempenho):** o número na parte inferior do gráfico exibe a latência mais baixa e o número na parte superior do gráfico exibe a latência mais alta para o período de 72 horas anterior. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor de latência para um tempo específico.

- Inferior (eventos):\* ao passar o Mouse, o pop-up exibe os detalhes dos eventos. Clique no link **Eventos ativos** abaixo do gráfico para navegar até a página Inventário de Eventos para exibir detalhes completos do evento.

#### • Gráfico do contador de IOPS

O gráfico do contador de IOPS fornece uma visão geral de alto nível da integridade do IOPS do objeto para o período de 72 horas anterior. IOPS indica a velocidade do sistema de armazenamento em número de operações de entrada/saída por segundo.

**Superior (valor do contador):** o número no cabeçalho exibe a média do período de 72 horas anterior.

**Médio (gráfico de desempenho):** o número na parte inferior do gráfico exibe o IOPS mais baixo, e o número na parte superior do gráfico exibe o IOPS mais alto para o período de 72 horas anterior. Posicione o cursor sobre a linha de tendência do gráfico para exibir o valor de IOPS para um tempo específico.

- Inferior (eventos):\* ao passar o Mouse, o pop-up exibe os detalhes dos eventos. Clique no link **Eventos ativos** abaixo do gráfico para navegar até a página Inventário de Eventos para exibir detalhes completos do evento.

#### • MB/s contador gráfico

O gráfico de contador MB/s exibe o desempenho do objeto MB/s e indica a quantidade de dados transferidos para e do objeto em megabytes por segundo. O gráfico de contador MB/s fornece uma visão geral de alto nível da integridade MB/s do objeto para o período de 72 horas anterior.

**Superior (valor do contador):** o número no cabeçalho exibe o número médio de MB/s para o período de 72 horas anterior.

**Médio (gráfico de desempenho):** o valor na parte inferior do gráfico exibe o menor número de MB/s, e o valor na parte superior do gráfico exibe o maior número de MB/s para o período de 72 horas anterior. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor MB/s para um tempo específico.

- Inferior (eventos):\* ao passar o Mouse, o pop-up exibe os detalhes dos eventos. Clique no link **Eventos ativos** abaixo do gráfico para navegar até a página Inventário de Eventos para exibir detalhes completos do evento.
- \* Tabela de contador usada capacidade de desempenho\*

O gráfico de contador capacidade de desempenho usada exibe a porcentagem de capacidade de desempenho que está sendo consumida pelo objeto.

**Superior (valor do contador):** o número no cabeçalho exibe a capacidade média de desempenho usada para o período de 72 horas anterior.

**Médio (gráfico de desempenho):** o valor na parte inferior do gráfico exibe a porcentagem de capacidade de desempenho mais baixa usada e o valor na parte superior do gráfico exibe a porcentagem de capacidade de desempenho mais alta usada para o período de 72 horas anterior. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor de capacidade de desempenho usado para um tempo específico.

- Inferior (eventos):\* ao passar o Mouse, o pop-up exibe os detalhes dos eventos. Clique no link **Eventos ativos** abaixo do gráfico para navegar até a página Inventário de Eventos para exibir detalhes completos do evento.
- **Gráfico do contador de utilização**

O gráfico do contador de utilização exibe a porcentagem de utilização do objeto. O gráfico do contador de utilização fornece uma visão geral de alto nível da porcentagem do objeto ou da utilização da largura de banda para o período de 72 horas anterior.

**Superior (valor do contador):** o número no cabeçalho exibe a porcentagem média de utilização para o período anterior de 72 horas.

**Médio (gráfico de desempenho):** o valor na parte inferior do gráfico exibe a porcentagem de utilização mais baixa e o valor na parte superior do gráfico exibe a porcentagem de utilização mais alta para o período de 72 horas anterior. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor de utilização para um tempo específico.

- Inferior (eventos):\* ao passar o Mouse, o pop-up exibe os detalhes dos eventos. Clique no link **Eventos ativos** abaixo do gráfico para navegar até a página Inventário de Eventos para exibir detalhes completos do evento.

## Eventos

A tabela de histórico de eventos, quando aplicável, lista os eventos mais recentes que ocorreram nesse objeto. Clicar no nome do evento exibe detalhes do evento na página Detalhes do evento.

## Componentes da página Performance Explorer

A página Performance Explorer permite comparar o desempenho de objetos semelhantes em um cluster - por exemplo, todos os volumes em um cluster. Isso é benéfico ao solucionar problemas de eventos de desempenho e ajustar o desempenho do objeto. Você também pode comparar objetos com o objeto raiz, que é a linha de base com a qual outras comparações de objetos são feitas.

Você pode clicar no botão **mudar para visualização de integridade** para exibir a página Detalhes de integridade para este objeto. Em alguns casos, você pode aprender informações importantes sobre as configurações de armazenamento para este objeto que podem ajudar ao solucionar um problema.

A página Explorador de desempenho exibe uma lista de objetos de cluster e seus dados de desempenho. Esta página exibe todos os objetos de cluster do mesmo tipo (por exemplo, volumes e suas estatísticas de desempenho específicas a objetos) em um formato tabular. Essa visualização fornece uma visão geral eficiente do desempenho do objeto de cluster.



Se "N/A" aparecer em qualquer célula da tabela, significa que um valor para esse contador não está disponível porque não há e/S nesse objeto neste momento.

A página Performance Explorer contém os seguintes componentes:

- **Intervalo de tempo**

Permite selecionar um intervalo de tempo para os dados do objeto.

Você pode escolher um intervalo predefinido ou especificar seu próprio intervalo de tempo personalizado.

- **Ver e comparar**

Permite-lhe selecionar qual o tipo de objeto correlacionado que é apresentado na grelha.

As opções disponíveis dependem do tipo de objeto raiz e seus dados disponíveis. Você pode clicar na lista suspensa Exibir e comparar para selecionar um tipo de objeto. O tipo de objeto selecionado é exibido na lista.

- **Filtragem**

Permite-lhe limitar a quantidade de dados que recebe, com base nas suas preferências.

Você pode criar filtros que se aplicam aos dados do objeto - por exemplo, IOPS maior que 4. Você pode adicionar até quatro filtros simultâneos.

- **Comparando**

Exibe uma lista dos objetos que você selecionou para comparação com o objeto raiz.

Os dados para os objetos no painel comparação são exibidos nos gráficos de Contador.

- **Exibir estatísticas em**

Para volume e LUNs, permite selecionar se as estatísticas são exibidas após cada ciclo de coleta (padrão de 5 minutos) ou se as estatísticas são mostradas como uma média horária. Essa funcionalidade permite que você visualize o gráfico de latência em suporte ao programa "Garantia de desempenho" da NetApp.

- **Gráficos de contador**

Exibe dados gráficos para cada categoria de desempenho de objeto.

Normalmente, apenas três ou quatro gráficos são exibidos por padrão. O componente escolher gráficos permite exibir gráficos adicionais ou ocultar gráficos específicos. Você também pode optar por mostrar ou ocultar a linha do tempo de Eventos.

- **Cronograma de Eventos**

Exibe eventos de desempenho e integridade que ocorrem na linha do tempo que você selecionou no componente intervalo de tempo.

## Gerenciando o desempenho usando informações de grupo de políticas de QoS

Com o Unified Manager, você pode visualizar os grupos de políticas de qualidade do serviço (QoS) disponíveis em todos os clusters que você está monitorando. As políticas podem ter sido definidas usando o software ONTAP (Gerenciador do sistema ou a CLI do ONTAP) ou por políticas de nível de serviço de performance do Unified Manager. O Unified Manager também exibe quais volumes e LUNs têm um grupo de políticas de QoS atribuído.

Para obter mais informações sobre como ajustar as configurações de QoS, consulte ["Visão geral do gerenciamento de desempenho"](#)

### Como a QoS do storage pode controlar a taxa de transferência de workload

Você pode criar um grupo de políticas de qualidade do serviço (QoS) para controlar o limite de e/S por segundo (IOPS) ou taxa de transferência (MB/s) para os workloads nele contidos. Se as cargas de trabalho estiverem em um grupo de políticas sem limite definido, como o grupo de políticas padrão ou o limite definido não atender às suas necessidades, você poderá aumentar o limite ou mover as cargas de trabalho para um grupo de políticas novo ou existente que tenha o limite desejado.

Os grupos de políticas de QoS "tradicionais" podem ser atribuídos a cargas de trabalho individuais, por exemplo, um único volume ou LUN. Nesse caso, a carga de trabalho pode usar o limite de taxa de transferência completa. Grupos de políticas de QoS também podem ser atribuídos a várias cargas de trabalho; nesse caso, o limite de taxa de transferência é "Vermelho" entre as cargas de trabalho. Por exemplo, um limite de QoS de 9.000 IOPS atribuído a três workloads restringiria o IOPS combinado de mais de 9.000 IOPS.

Os grupos de política de QoS "adaptável" também podem ser atribuídos a workloads individuais ou vários workloads. No entanto, mesmo quando atribuído a vários workloads, cada workload recebe o limite de taxa de transferência completa em vez de compartilhar o valor da taxa de transferência com outros workloads. Além disso, as políticas de QoS adaptáveis ajustam automaticamente a configuração de taxa de transferência com base no tamanho do volume, por workload, mantendo a proporção de IOPS para terabytes à medida que o tamanho do volume muda. Por exemplo, se o pico estiver definido para 5.000 IOPS/TB em uma política de QoS adaptável, um volume de 10 TB terá uma taxa de transferência máxima de 50.000 IOPS. Se o volume for redimensionado posteriormente para 20 TB, a QoS adaptável ajusta o máximo para 100.000 IOPS.

A partir do ONTAP 9.5, você pode incluir o tamanho do bloco ao definir uma política de QoS adaptável. Isso converte efetivamente a política de um limite de IOPS/TB para um limite de MB/s para casos em que as cargas de trabalho estão usando tamanhos de bloco muito grandes e, em última análise, usando uma grande porcentagem de taxa de transferência.

Para políticas de QoS de grupo compartilhado, quando o IOPS ou MB/s de todos os workloads em um grupo de políticas excede o limite definido, o grupo de políticas mantém os workloads para restringir a atividade, o que pode diminuir a performance de todos os workloads no grupo de políticas. Se um evento de desempenho dinâmico for gerado pela limitação do grupo de políticas, a descrição do evento exibirá o nome do grupo de políticas envolvido.

Na exibição desempenho: Todos os volumes, você pode classificar os volumes afetados por IOPS e MB/s para ver quais cargas de trabalho têm o maior uso que pode ter contribuído para o evento. Na página Performance/volumes Explorer, é possível selecionar outros volumes ou LUNs no volume para comparar com o uso de IOPS do workload afetado ou taxa de transferência em Mbps.

Ao atribuir as cargas de trabalho que estão sobreusando os recursos do nó a uma configuração de grupo de políticas mais restritiva, o grupo de políticas mantém as cargas de trabalho para restringir sua atividade, o que pode reduzir o uso dos recursos nesse nó. No entanto, se você quiser que a carga de trabalho possa usar mais recursos do nó, você pode aumentar o valor do grupo de políticas.

Você pode usar o Gerenciador de sistema, os comandos do ONTAP ou os níveis de Serviço de Performance do Gerenciador Unificado para gerenciar grupos de políticas, incluindo as seguintes tarefas:

- Criando um grupo de políticas
- Adição ou remoção de cargas de trabalho em um grupo de políticas
- Movimentação de uma carga de trabalho entre grupos de políticas
- Alterar o limite de taxa de transferência de um grupo de políticas
- Mover um workload para um agregado e/ou nó diferente


## Visualização de todos os grupos de políticas de QoS disponíveis em todos os clusters

É possível exibir uma lista de todos os grupos de políticas de QoS disponíveis nos clusters que o Unified Manager está monitorando. Isso inclui políticas tradicionais de QoS, políticas de QoS adaptáveis e políticas de QoS gerenciadas por políticas de nível de serviço de performance do Unified Manager.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > QoS Policy Groups**.

A exibição desempenho: Grupos de políticas de QoS tradicionais é exibida por padrão.

2. Visualize as configurações detalhadas de cada grupo de políticas de QoS tradicional disponível.
3. Clique no botão expandir (  ) ao lado do nome do grupo de políticas de QoS para ver mais detalhes sobre o grupo de políticas.
4. No menu Exibir, selecione uma das opções adicionais para exibir todos os grupos de políticas de QoS adaptáveis ou para exibir todos os grupos de políticas de QoS criados usando níveis de Serviço de desempenho do Unified Manager.

## Exibindo volumes ou LUNs que estão no mesmo grupo de políticas de QoS

É possível exibir uma lista dos volumes e LUNs atribuídos ao mesmo grupo de políticas de QoS.


No caso de grupos de políticas de QoS tradicionais que são "compartilhados" entre vários volumes, isso pode ser útil para ver se certos volumes estão sobreusando o throughput definido para o grupo de políticas. Ele também pode ajudá-lo a decidir se você pode adicionar outros volumes ao grupo de políticas sem afetar negativamente os outros volumes.

No caso de políticas de QoS adaptáveis e políticas de níveis de Serviço de Performance do Unified Manager, isso pode ser útil para exibir todos os volumes ou LUNs que estão usando um grupo de políticas, para que você possa ver quais objetos seriam afetados se você alterou as configurações da política de QoS.


### Passos

1. No painel de navegação esquerdo, clique em **Storage > QoS Policy Groups**.



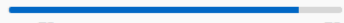


A exibição desempenho: Grupos de políticas de QoS tradicionais é exibida por padrão.

2. Se você está interessado em grupo político tradicional, fique nesta página. Caso contrário, selecione uma das opções de visualização adicionais para exibir todos os grupos de políticas de QoS adaptáveis ou todos os grupos de políticas de QoS criados pelos níveis de Serviço de desempenho do Unified Manager.
3. Na política de QoS em que você está interessado, clique no botão expandir (  ) ao lado do nome do grupo de políticas de QoS para exibir mais detalhes.

Quality of Service - Performance / Adaptive QoS Policy Groups 

Last updated: Jan 31, 2019, 1:56 PM 

View Adaptive QoS Policy Groups

QoS Policy Group	Cluster	SVM	Min Through...	Max Through...	Absolute Min...	Block Size	Asso
 julia_vs2_cifs_Performance	opm-simplicity	julia_vs2_cifs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		1
 julia_vs1_nfs_Performance	opm-simplicity	julia_vs1_nfs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		2
<b>Details</b> Allocated Capacity  0.99 TB / 1.15 TB Associated Objects <span>2 Volumes</span> <span>0 LUNs</span> Events None							
 julia_nfs_extreme_Extreme_Performance	ocum-mobility-01-02	julia_nfs_extreme	6144.0 IOPS/TB	12288.0 IOPS/TB	1000IOPS	any	1
 julia_extreme_jan16_aqos	ocum-mobility-01-02	julia_nfs_extreme	10000.0 IOPS/TB	12000.0 IOPS/TB	1000IOPS	any	1

4. Clique no link volumes ou LUNs para exibir os objetos usando essa política de QoS.

A página de inventário de desempenho para volumes ou LUNs é exibida com a lista ordenada de objetos que estão usando a política de QoS.

## Exibindo as configurações do grupo de políticas de QoS aplicadas a volumes ou LUNs específicos

Você pode exibir os grupos de políticas de QoS que foram aplicados aos volumes e



LUNs e pode vincular a exibição grupos de políticas de desempenho/QoS para exibir as configurações detalhadas de cada política de QoS.

As etapas para exibir a política de QoS aplicada a um volume são mostradas abaixo. As etapas para exibir essas informações para um LUN são semelhantes.

#### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.

A exibição Saúde: Todos os volumes é exibida por padrão.

2. No menu Exibir, selecione **desempenho: Volumes no Grupo de políticas QoS**.
3. Localize o volume que deseja revisar e role para a direita até ver a coluna **Grupo de políticas QoS**.
4. Clique no nome do grupo de políticas de QoS.

A página qualidade do serviço correspondente é exibida dependendo se é uma política de QoS tradicional, uma política de QoS adaptável ou uma política de QoS criada usando os níveis de serviço de desempenho do Unified Manager.

5. Exiba as configurações detalhadas do grupo de políticas de QoS.
6. Clique no botão expandir (▼) ao lado do nome do grupo de políticas de QoS para ver mais detalhes sobre o grupo de políticas.

### Exibição de gráficos de desempenho para comparar volumes ou LUNs que estão no mesmo grupo de políticas de QoS

Você pode visualizar os volumes e LUNs que estão nos mesmos grupos de política de QoS e, em seguida, comparar o desempenho em um único gráfico de IOPS, MB/s ou IOPS/TB para identificar quaisquer problemas.

As etapas para comparar o desempenho de volumes no mesmo grupo de políticas de QoS são mostradas abaixo. As etapas para exibir essas informações para um LUN são semelhantes.

#### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.

A exibição Saúde: Todos os volumes é exibida por padrão.

2. No menu Exibir, selecione **desempenho: Volumes no Grupo de políticas QoS**.
3. Clique no nome do volume que você deseja revisar.

A página do Explorador de desempenho é apresentada para o volume.

4. No menu Exibir e comparar, selecione **volumes no mesmo Grupo de políticas de QoS**.

Os outros volumes que compartilham a mesma política de QoS estão listados na tabela abaixo.

5. Clique no botão **Adicionar** para adicionar esses volumes aos gráficos para que você possa comparar os contadores de IOPS, MB/s, IOPS/TB e outros contadores de desempenho de todos os volumes selecionados nos gráficos.

Pode alterar o intervalo de tempo para ver o desempenho em diferentes intervalos de tempo, exceto o

padrão de 72 horas.

## Como diferentes tipos de políticas de QoS são exibidos nos gráficos de taxa de transferência

Você pode exibir as configurações de política de qualidade do serviço (QoS) definidas pelo ONTAP que foram aplicadas a um volume ou LUN nos gráficos de desempenho e análise de carga de trabalho IOPS, IOPS/TB e MB/s. As informações exibidas nos gráficos são diferentes dependendo do tipo de política de QoS que foi aplicada à carga de trabalho.

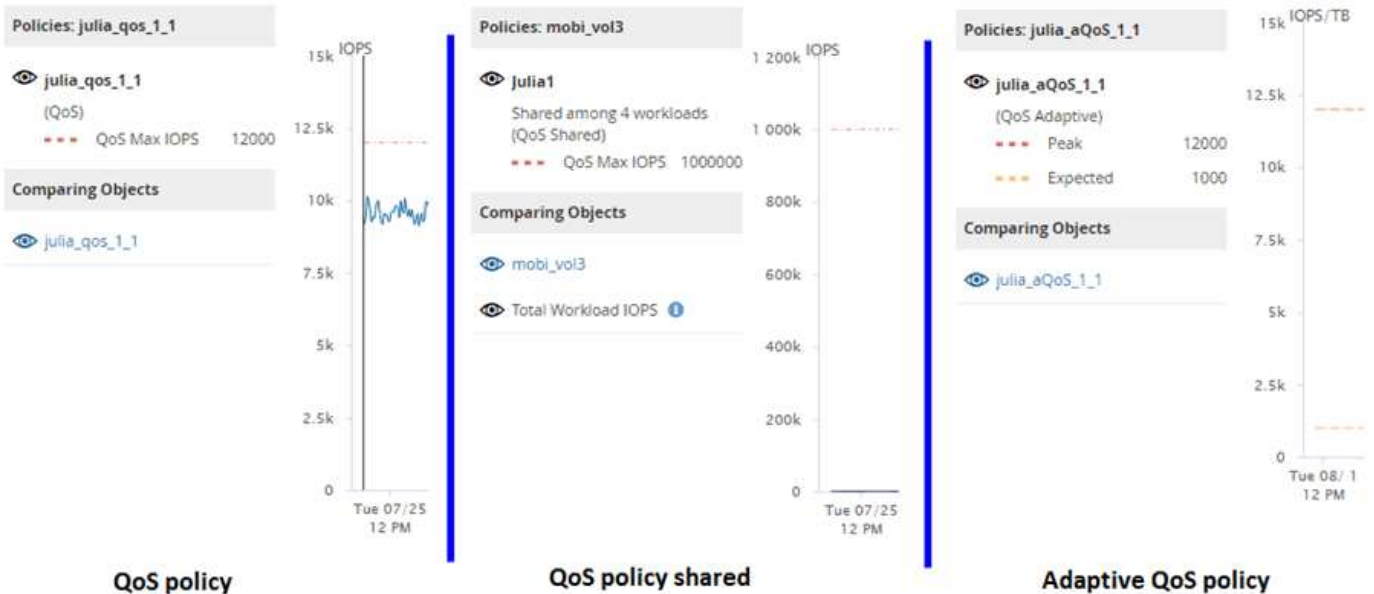
Uma configuração de taxa de transferência máxima (ou "pico") define a taxa de transferência máxima que a carga de trabalho pode consumir e, assim, limita o impacto nas cargas de trabalho da concorrência para recursos do sistema. Uma configuração mínima de taxa de transferência (ou "esperada") define a taxa de transferência mínima que deve estar disponível para a carga de trabalho de modo que uma carga de trabalho crítica atenda aos destinos mínimos de taxa de transferência, independentemente da demanda por cargas de trabalho concorrentes.

As políticas de QoS compartilhadas e não compartilhadas para IOPS e MB/s usam os termos "Mínimo" e "Máximo" para definir o piso e o teto. As políticas adaptativas de QoS para IOPS/TB, que foram introduzidas no ONTAP 9.3, usam os termos "esperado" e "pico" para definir o piso e o teto.

Embora o ONTAP permita que você crie esses dois tipos de políticas de QoS, dependendo de como eles são aplicados a workloads, há três maneiras de que a política de QoS será exibida nos gráficos de performance.

Tipo de política	Funcionalidade	Indicador na interface do Unified Manager
Política compartilhada de QoS atribuída a um único workload ou política de QoS não compartilhada atribuída a um único workload ou a vários workloads	Cada workload pode consumir a configuração de taxa de transferência especificada	Exibe "(QoS)"
Política compartilhada de QoS atribuída a vários workloads	Todos os workloads compartilham a configuração de taxa de transferência especificada	Exibe "(QoS compartilhado)"
Política de QoS adaptável atribuída a um único workload ou vários workloads	Cada workload pode consumir a configuração de taxa de transferência especificada	Exibe "(QoS Adaptive)"

A figura a seguir mostra um exemplo de como as três opções são mostradas nos gráficos de contador.



Quando uma política de QoS normal que foi definida em IOPS aparece no gráfico IOPS/TB para um workload, o ONTAP converte o valor de IOPS/TB em um valor de IOPS/TB e o Unified Manager exibe essa política no gráfico IOPS/TB juntamente com o texto "QoS, definido em IOPS".

Quando uma política de QoS adaptável que foi definida em IOPS/TB aparece no gráfico de IOPS para uma carga de trabalho, o ONTAP converte o valor de IOPS/TB em um valor de IOPS e o Unified Manager exibe essa política no gráfico de IOPS juntamente com o texto "QoS adaptável - usado, definido em IOPS/TB" ou "Adaptativo - alocado, definido em IOPS/TB" dependendo de como a configuração de alocação de QoS de pico é configurada. Quando a configuração de alocação é definida como "espaço alocado", o IOPS de pico é calculado com base no tamanho do volume. Quando a configuração de alocação é definida como "espaço usado", o IOPS de pico é calculado com base na quantidade de dados armazenados no volume, levando em conta as eficiências de armazenamento.



O gráfico IOPS/TB exibe dados de desempenho somente quando a capacidade lógica usada pelo volume é maior ou igual a 128 GB. As lacunas são exibidas no gráfico quando a capacidade usada cai abaixo de 128 GB durante o período de tempo selecionado.

## Exibindo configurações mínimas e máximas de QoS do workload no Performance Explorer

Você pode exibir as configurações de política de qualidade do serviço (QoS) definidas pelo ONTAP em um volume ou LUN nos gráficos do Explorador de desempenho. Uma configuração máxima de taxa de transferência limita o impacto das cargas de trabalho da concorrência nos recursos do sistema. Uma configuração mínima de taxa de transferência garante que um workload crítico atenda aos destinos mínimos de taxa de transferência, independentemente da demanda por workloads da concorrência.

As configurações de IOPS e MB/s são exibidas nos gráficos de contador somente se tiverem sido configurados no ONTAP. As configurações mínimas de taxa de transferência estão disponíveis somente em sistemas que executam o ONTAP 9.2 ou software posterior, somente em sistemas AFF, e elas podem ser definidas somente para IOPS neste momento.

As políticas de QoS adaptáveis estão disponíveis a partir do ONTAP 9.3 e são expressas usando IOPS/TB em vez de IOPS. Essas políticas ajustam automaticamente o valor da política de QoS com base no tamanho

do volume, por workload, mantendo assim a proporção de IOPS para terabytes à medida que o tamanho do volume muda. Você pode aplicar um grupo de políticas de QoS adaptável apenas a volumes. A terminologia de QoS "esperado" e "pico" são usadas para políticas de QoS adaptáveis em vez de mínima e máxima.

O Unified Manager gera eventos de aviso para violações de política de QoS quando a taxa de transferência de workload excedeu a configuração de política máxima de QoS definida durante cada período de coleta de performance da hora anterior. A taxa de transferência do workload pode exceder o limite de QoS por apenas um curto período de tempo durante cada período de coleta, mas o Unified Manager exibe a taxa de transferência "média" durante o período de coleta no gráfico. Por esse motivo, você pode ver eventos de QoS enquanto a taxa de transferência de um workload pode não ter cruzado o limite de política mostrado no gráfico.

## Passos

1. Na página **Explorador de desempenho** do volume ou LUN selecionado, execute as seguintes ações para visualizar as definições do teto e do piso de QoS:

Se você quiser...	Faça isso...
Ver o teto de IOPS (o QoS máximo)	No gráfico Total de IOPS ou Breakdown, clique em <b>Zoom View</b> .
Ver o teto MB/s (o máximo QoS)	No gráfico total de MB/s ou de divisão, clique em <b>Zoom View</b> .
Ver o piso de IOPS (o QoS min)	No gráfico Total de IOPS ou Breakdown, clique em <b>Zoom View</b> .
Visualizar o limite de IOPS/TB (o pico de QoS)	Para volumes, no gráfico IOPS/TB, clique em <b>Zoom View</b> .
Visualizar o piso de IOPS/TB (a QoS esperada)	Para volumes, no gráfico IOPS/TB, clique em <b>Zoom View</b> .

A linha horizontal tracejada indica o valor máximo ou mínimo da taxa de transferência definido no ONTAP. Você também pode exibir quando as alterações nos valores de QoS foram implementadas.

2. Para exibir os valores de IOPS e MB/s específicos em comparação com a configuração de QoS, mova o cursor para a área do gráfico para ver a janela pop-up.

Se você notar que certos volumes ou LUNs têm IOPS ou MB/s muito altos e estão estressando os recursos do sistema, use o Gerenciador do sistema ou a CLI da ONTAP para ajustar as configurações de QoS de modo que esses workloads não afetem a performance de outros workloads.

Para obter mais informações sobre como ajustar as configurações de QoS, consulte ["Visão geral do gerenciamento de desempenho"](#)

## Gerenciamento da performance com a capacidade de performance e as informações de IOPS disponíveis

*Capacidade de desempenho* indica quanto throughput você pode obter de um recurso sem superar o desempenho útil desse recurso. Quando vista usando contadores de

performance existentes, a capacidade de performance é o ponto em que você obtém a utilização máxima de um nó ou agregado antes que a latência se torne um problema.

O Unified Manager coleta estatísticas de capacidade de performance de nós e agregados em cada cluster. *Capacidade de desempenho usada* é a porcentagem de capacidade de desempenho que está sendo usada atualmente, e *capacidade de desempenho livre* é a porcentagem de capacidade de desempenho que ainda está disponível.

Embora a capacidade de desempenho livre forneça uma porcentagem do recurso que ainda está disponível, *IOPS disponível* informa o número de IOPS que podem ser adicionados ao recurso antes de atingir a capacidade máxima de desempenho. Usando essa métrica, você pode ter certeza de que pode adicionar workloads de um número predeterminado de IOPS a um recurso.

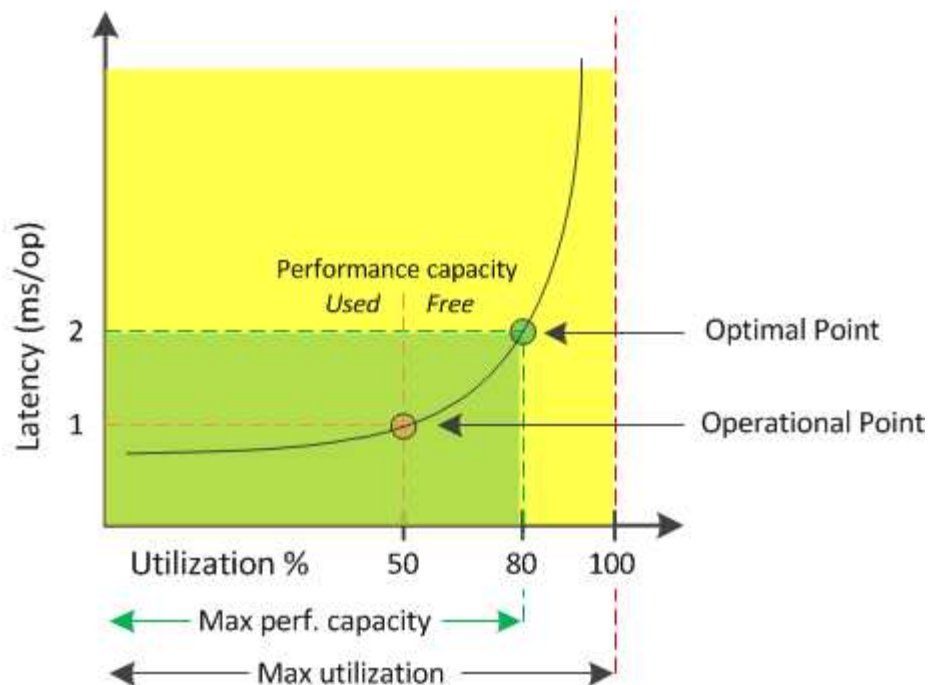
O monitoramento das informações de capacidade de desempenho tem os seguintes benefícios:

- Auxilia no provisionamento e balanceamento de fluxo de trabalho.
- Ajuda a evitar sobrecarregar um nó ou empurrar seus recursos para além do ponto ideal, reduzindo assim a necessidade de solucionar problemas.
- Ajuda você a determinar com maior precisão onde equipamentos de armazenamento adicionais podem ser necessários.

## **Qual é a capacidade de desempenho utilizada**

O contador de capacidade de desempenho usado ajuda a identificar se o desempenho de um nó ou de um agregado está atingindo um ponto em que o desempenho pode degradar se as cargas de trabalho aumentarem. Ele também pode mostrar se um nó ou agregado está sendo usado em excesso durante períodos específicos de tempo. A capacidade de performance usada é semelhante à utilização, mas a primeira fornece mais informações sobre os recursos de performance disponíveis em um recurso físico para uma carga de trabalho específica.

A capacidade de performance usada ideal é o ponto em que um nó ou um agregado tem utilização e latência ideais (tempo de resposta) e está sendo usado com eficiência. Uma curva de latência versus utilização de amostra é mostrada para um agregado na figura a seguir.



Neste exemplo, o *ponto operacional* identifica que o agregado está operando atualmente em 50% de utilização com latência de 1,0 ms/op. Com base nas estatísticas capturadas do agregado, o Unified Manager determina que a capacidade de desempenho adicional está disponível para esse agregado. Neste exemplo, o *ponto ótimo* é identificado como o ponto quando o agregado está em 80% de utilização com latência de 2,0 ms/op. Portanto, é possível adicionar mais volumes e LUNs a esse agregado para que seus sistemas sejam usados com mais eficiência.

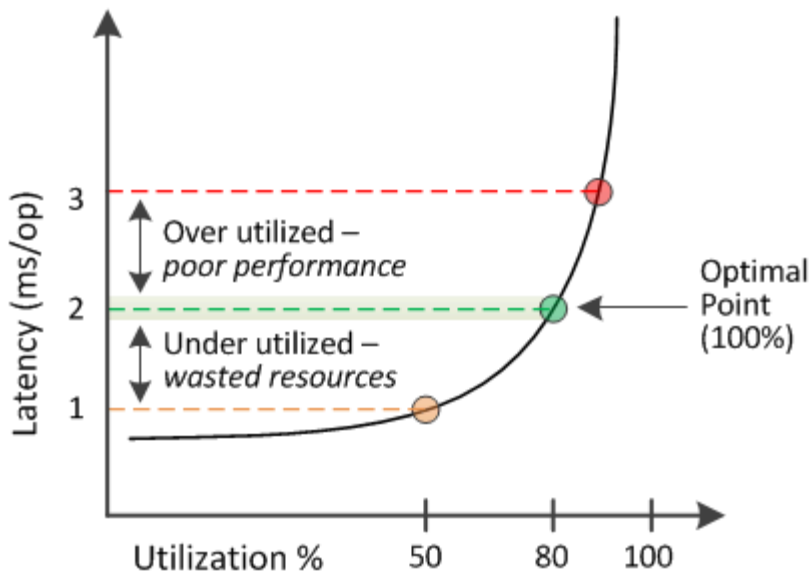
Espera-se que o contador de capacidade de desempenho usado seja um número maior do que o contador de "utilização" porque a capacidade de desempenho aumenta o impactos na latência. Por exemplo, se um nó ou agregado for 70% usado, o valor da capacidade de desempenho pode estar na faixa de 80% a 100%, dependendo do valor de latência.

Em alguns casos, no entanto, o contador de utilização pode ser superior na página Painel de instrumentos. Isso é normal porque o painel atualiza os valores atuais do contador em cada período de coleta; ele não exibe médias em um período de tempo, como as outras páginas na interface de usuário do Unified Manager. O contador de capacidade de desempenho usado é melhor usado como um indicador de desempenho médio ao longo de um período de tempo, enquanto o contador de utilização é melhor usado para determinar o uso instantâneo de um recurso.

## O que significa o valor da capacidade de desempenho utilizada

O valor da capacidade de desempenho usado ajuda a identificar os nós e agregados que estão sendo sobreutilizados ou subutilizados atualmente. Isso permite redistribuir workloads para aumentar a eficiência dos recursos de storage.

A figura a seguir mostra a curva de latência versus utilização de um recurso e identifica, com pontos coloridos, três áreas onde o ponto operacional atual poderia estar localizado.



- Uma percentagem de capacidade de desempenho usada igual a 100 está no ponto ideal.

Os recursos estão sendo usados de forma eficiente neste momento.

- Uma percentagem de capacidade de desempenho usada acima de 100 indica que o nó ou o agregado está sobreutilizado e que as cargas de trabalho estão recebendo desempenho abaixo do ideal.

Nenhuma nova carga de trabalho deve ser adicionada ao recurso, e as cargas de trabalho existentes podem precisar ser redistribuídas.

- Uma percentagem de capacidade de desempenho usada abaixo de 100 indica que o nó ou o agregado está subutilizado e que os recursos não estão sendo usados com eficiência.

Mais workloads podem ser adicionados ao recurso.



Diferentemente da utilização, a percentagem de capacidade de performance usada pode estar acima de 100%. Não há percentagem máxima, mas os recursos geralmente estarão na faixa de 110% a 140% quando estiverem sendo sobreutilizados. Percentagens mais elevadas indicariam um recurso com problemas graves.

## O que é IOPS disponível

O contador de IOPS disponível identifica o número restante de IOPS que pode ser adicionado a um nó ou a um agregado antes que o recurso atinja seu limite.

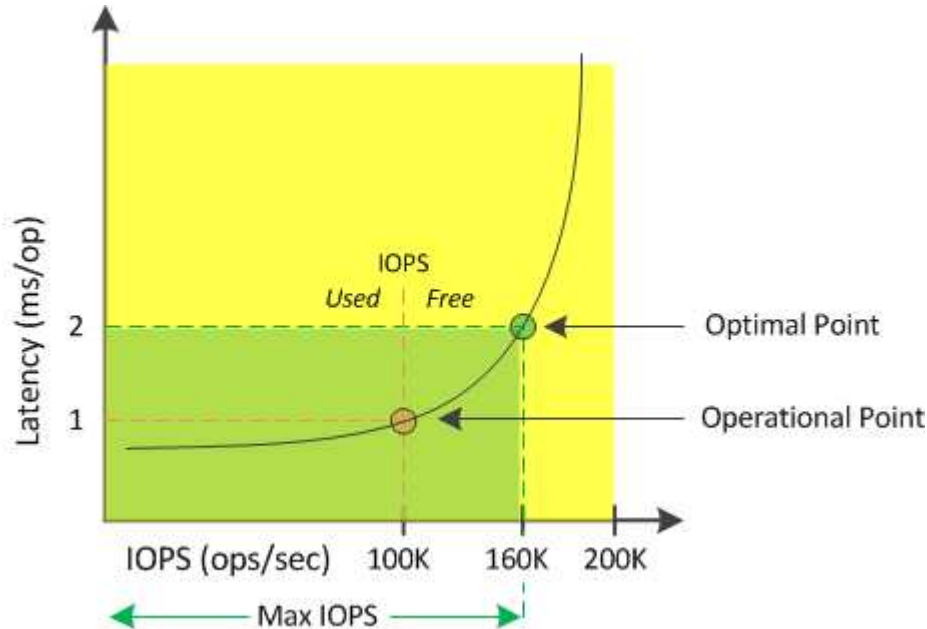
O total de IOPS que um nó pode fornecer é baseado nas características físicas do nó - por exemplo, o número de CPUs, a velocidade da CPU e a quantidade de RAM. O total de IOPS que um agregado pode fornecer é baseado nas propriedades físicas dos discos - por exemplo, um disco SATA, SAS ou SSD.

O total de IOPS de todos os volumes em um agregado pode não corresponder ao total de IOPS do agregado. Isso é discutido no seguinte artigo da base de conhecimento: [KB "Por que a soma de todos os IOPs de volume em um agregado não corresponde aos IOPs agregados?"](#)

Embora o contador de capacidade de performance forneça a percentagem de um recurso que ainda está disponível, o contador de IOPS disponível informa o número exato de IOPS (cargas de trabalho) pode ser adicionado a um recurso antes de atingir a capacidade máxima de performance.

Por exemplo, se você estiver usando um par de sistemas de storage FAS2520 e FAS8060, um valor sem capacidade de performance de 30% significa que você tem alguma capacidade de performance gratuita. No entanto, esse valor não fornece visibilidade sobre o número de workloads que você pode implantar nesses nós. O contador de IOPS disponível pode mostrar que você tem 500 IOPS disponíveis no FAS8060, mas apenas 100 IOPS disponíveis no FAS2520.

Uma curva de latência de exemplo versus IOPS para um nó é mostrada na figura a seguir.



O número máximo de IOPS que um recurso pode fornecer é o número de IOPS quando o contador de capacidade de desempenho usado é de 100% (o ponto ideal). O ponto operacional identifica que o nó está operando atualmente em 100K IOPS com latência de 1,0 ms/op. Com base nas estatísticas capturadas a partir do nó, o Unified Manager determina que o máximo de IOPS para o nó é 160K, o que significa que há 60K IOPS livres ou disponíveis. Portanto, você pode adicionar mais workloads a esse nó para que seus sistemas sejam usados com mais eficiência.



Quando há uma atividade mínima do usuário no recurso, o valor de IOPS disponível é calculado assumindo uma carga de trabalho genérica com base em aproximadamente 4.500 IOPS por núcleo da CPU. Isso ocorre porque o Unified Manager não tem os dados para estimar com precisão as características da carga de trabalho que está sendo atendida.

## Exibindo valores de capacidade de desempenho agregado e nó usados

Você pode monitorar os valores de capacidade de performance usados para todos os nós ou para todos os agregados em um cluster, ou visualizar detalhes de um único nó ou agregado.

Os valores de capacidade de desempenho usados são exibidos no Painel, nas páginas de inventário de desempenho, na página de principais artistas, na página criar política de limite, nas páginas do Performance Explorer e nos gráficos detalhados. Por exemplo, a página desempenho: Todos os agregados fornece uma coluna capacidade de desempenho usada para exibir o valor da capacidade de desempenho usada para todos os agregados.



Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used ↓	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
✓	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
✓	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
✓	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
✓	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
✓	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
✓	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
✓	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
✓	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS
⚠	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS

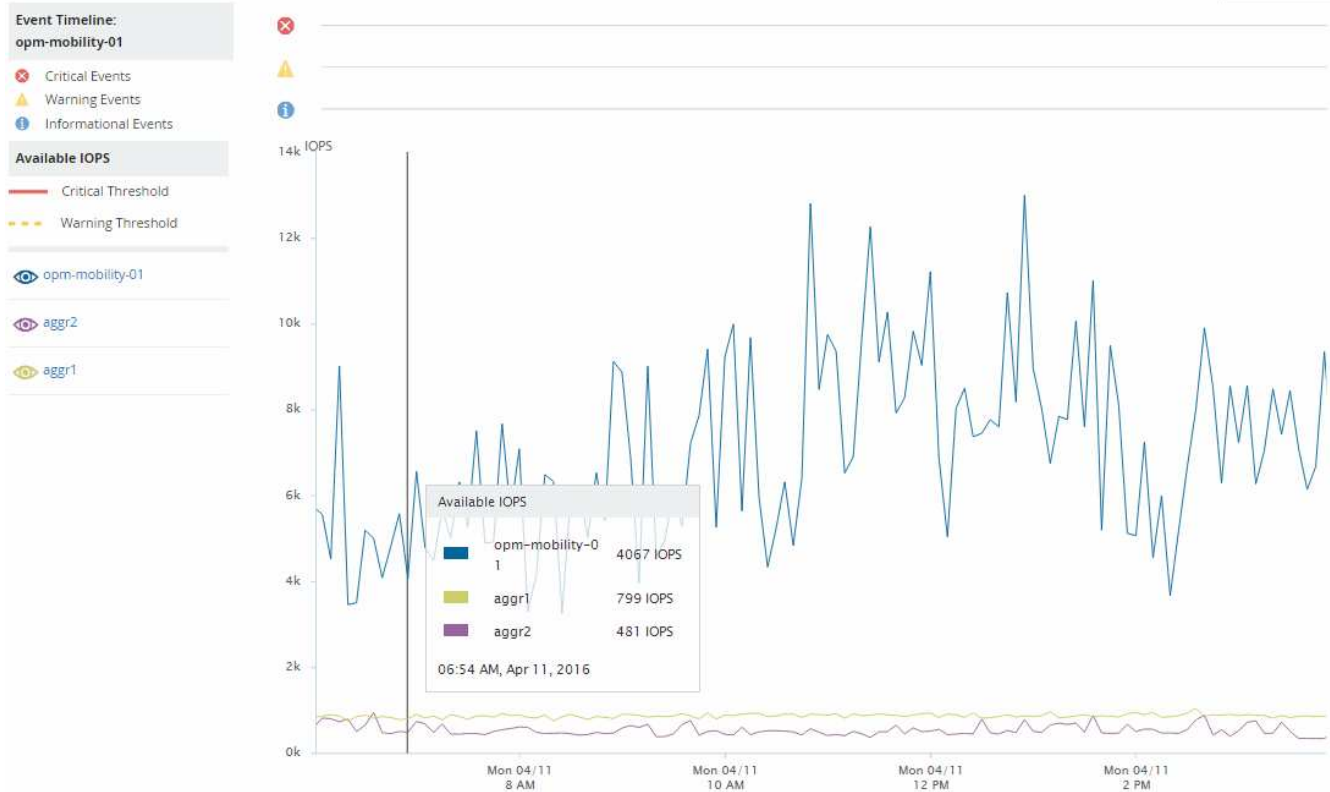
O monitoramento do contador de capacidade de desempenho usado permite identificar o seguinte:

- Independentemente de nós ou agregados em qualquer cluster terem um valor usado de alta capacidade de performance
- Mesmo que nós ou agregados em qualquer cluster tenham eventos usados de capacidade de performance ativa
- Os nós e agregados que têm o valor mais alto e mais baixo da capacidade de performance usada em um cluster
- Valores de contador de latência e utilização em conjunto com nós ou agregados que têm valores de capacidade de alta performance usados
- Como os valores da capacidade de performance usada para nós em um par de HA serão afetados se um dos nós falhar
- Os volumes e LUNs mais ativos em um agregado que tenha um valor de capacidade de alta performance usada

## Exibindo o nó e agregar valores de IOPS disponíveis

Você pode monitorar os valores de IOPS disponíveis para todos os nós ou para todos os agregados em um cluster, ou visualizar detalhes de um único nó ou agregado.

Os valores de IOPS disponíveis aparecem nas páginas Inventário de desempenho e nos gráficos de páginas do Performance Explorer para nós e agregados. Por exemplo, ao visualizar um nó na página do Explorador de nó/desempenho, você pode selecionar o gráfico de contador "Available IOPS" na lista para comparar os valores de IOPS disponíveis para o nó e vários agregados nesse nó.



O monitoramento do contador de IOPS disponível permite identificar:

- Nós ou agregados que têm os maiores valores de IOPS disponíveis para ajudar a determinar onde workloads futuros podem ser implantados.
- Os nós ou agregados que têm os menores valores de IOPS disponíveis para identificar os recursos que você deve monitorar para possíveis problemas de desempenho futuros.
- Os volumes e LUNs mais ativos em um agregado que tenha um pequeno valor de IOPS disponível.

## Visualização de gráficos de contadores de capacidade de desempenho para identificar problemas

Você pode visualizar gráficos usados de capacidade de performance para nós e agregados na página Performance Explorer. Isso permite visualizar dados detalhados de capacidade de performance para os nós selecionados e agregados para um período de tempo específico.

O gráfico de contador padrão exibe os valores de capacidade de desempenho usados para os nós ou agregados selecionados. O gráfico de contador de avarias exibe os valores de capacidade de desempenho total para o objeto raiz separado em uso com base em protocolos de usuário versus processos de sistema em segundo plano. Além disso, a quantidade de capacidade de desempenho livre também é mostrada.

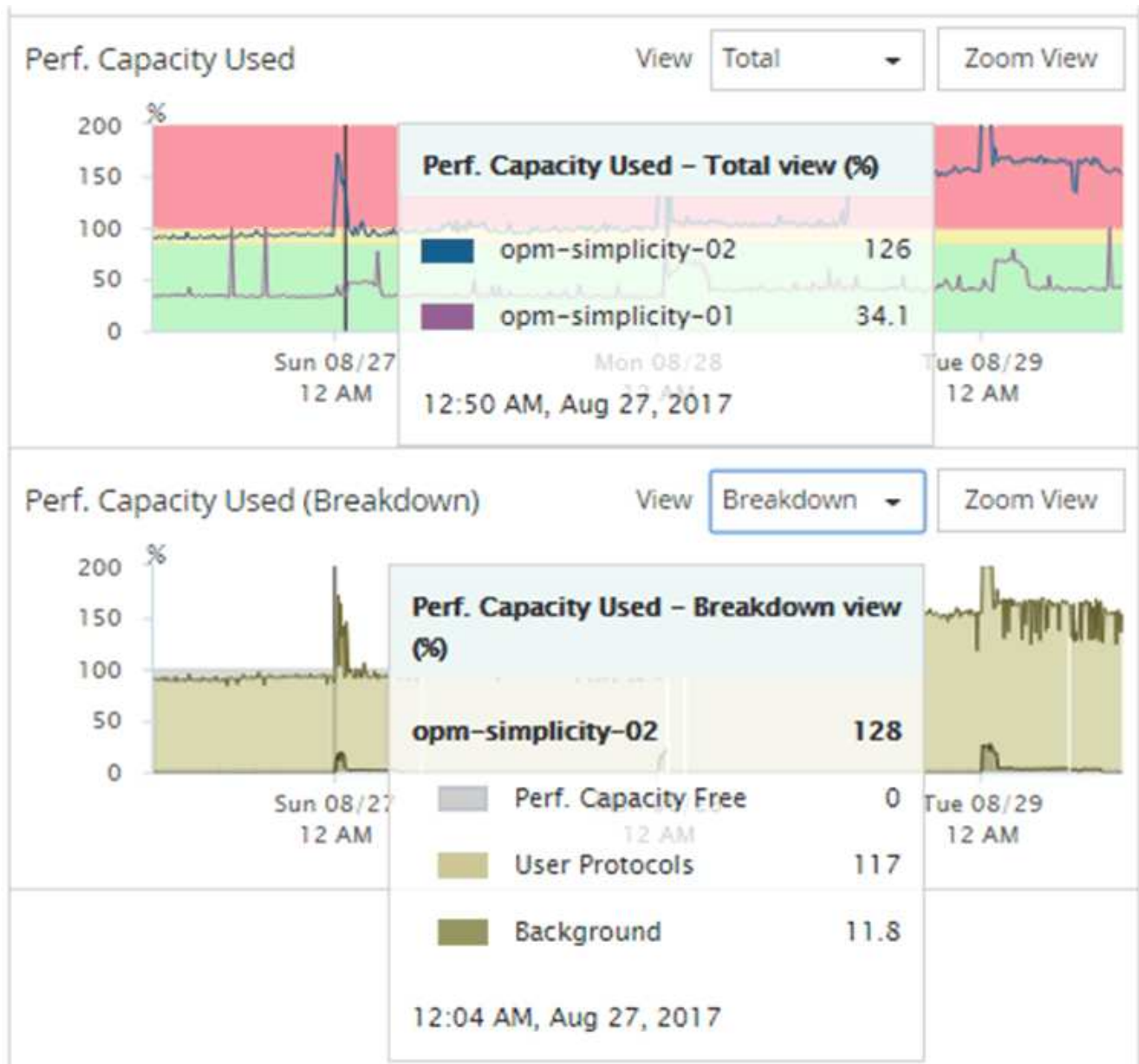


Como algumas atividades em segundo plano associadas ao gerenciamento de dados e sistema são identificadas como cargas de trabalho do usuário e categorizadas como protocolos de usuário, a porcentagem de protocolos do usuário pode parecer artificialmente alta quando esses processos são executados. Esses processos normalmente são executados por volta da meia-noite quando o uso do cluster é baixo. Se você vir um pico na atividade do protocolo do usuário por volta da meia-noite, verifique se os trabalhos de backup do cluster ou outras atividades em segundo plano estão configurados para serem executados nesse momento.

### Passos

1. Selecione a guia **Explorer** de um nó ou agregue a página **Landing**.
2. No painel **Counter Charts**, clique em **Choose charts** e selecione **Perf. Gráfico de capacidade utilizada**.
3. Role para baixo até que você possa visualizar o gráfico.

As cores do gráfico padrão mostram quando o objeto está no intervalo ideal (amarelo), quando o objeto está subutilizado (verde) e quando o objeto é sobreutilizado (vermelho). O gráfico de detalhamento mostra detalhes detalhados da capacidade de desempenho somente para o objeto raiz.



4. Se você quiser exibir qualquer gráfico em um formato completo, clique em **Zoom View**.

Dessa forma, você pode abrir vários gráficos de contador em uma janela separada para comparar os valores de capacidade de desempenho usados com valores de IOPS ou Mbps no mesmo período de tempo.

## Condições de limite de performance usadas pela capacidade de performance

Você pode criar políticas de limite de performance definidas pelo usuário para que os eventos sejam acionados quando o valor de capacidade de performance usada para um nó ou agregado exceder a configuração de limite de capacidade de performance definida.

Além disso, os nós podem ser configurados com uma política de limite de capacidade de desempenho usada de aquisição. Essa política de limite totaliza as estatísticas de capacidade de performance usadas para ambos os nós em um par de HA para determinar se um dos nós não teria capacidade suficiente se o outro nó falhar. Como a carga de trabalho durante o failover é a combinação das cargas de trabalho dos dois nós parceiros, a mesma capacidade de performance usada política de takeover pode ser aplicada a ambos os nós.



Essa capacidade de desempenho utilizada é geralmente verdadeira entre nós. No entanto, se houver significativamente mais tráfego entre nós destinado a um dos nós por meio de seu parceiro de failover, a capacidade total de performance usada ao executar todos os workloads em um nó de parceiro em vez do outro nó de parceiro poderá ser um pouco diferente, dependendo de qual nó tiver falhado.

As condições de capacidade de performance usadas também podem ser usadas como configurações de limite de performance secundário para criar uma política de limite de combinação ao definir limites para LUNs e volumes. A condição de capacidade de desempenho usada é aplicada ao agregado ou nó no qual reside o volume ou LUN. Por exemplo, você pode criar uma política de limite de combinação usando os seguintes critérios:

Objeto de storage	Contador de desempenho	Limite de aviso	Limite crítico	Duração
Volume	Latência	15 ms/op	25 ms/op	20 minutos
Agregado	Capacidade de performance utilizada	80%	95%	

As políticas de limite de combinação fazem com que um evento seja gerado somente quando ambas as condições forem violadas durante toda a duração.

## Usando o contador de capacidade de desempenho usado para gerenciar o desempenho

Em geral, as organizações querem operar com uma porcentagem de capacidade de performance usada abaixo de 100 para que os recursos estejam sendo usados com eficiência, reservando alguma capacidade de performance adicional para atender às demandas do período de pico. Você pode usar políticas de limite para personalizar

quando os alertas são enviados para valores usados de capacidade de alta performance.

Você pode estabelecer metas específicas com base em seus requisitos de performance. Por exemplo, as empresas de serviços financeiros podem reservar mais capacidade de desempenho para garantir a execução oportuna de negociações. Essas empresas podem querer definir limites de capacidade de desempenho usados na faixa de 70-80%. Empresas de manufatura com margens menores podem optar por reservar menos capacidade de desempenho se estiverem dispostas a arriscar o desempenho para gerenciar melhor os custos DE TI. Essas empresas podem definir limites de capacidade de desempenho usados na faixa de 85-95%.

Quando o valor da capacidade de performance usada excede a porcentagem definida em uma política de limite definida pelo usuário, o Unified Manager envia um e-mail de alerta e adiciona o evento à página Inventário de Eventos. Isso permite que você gerencie possíveis problemas antes que eles afetem o desempenho. Esses eventos também podem ser usados como indicadores de que você precisa para fazer mudanças e mudanças de workload em seus nós e agregados.

## **Compreender e utilizar a página Planejamento de failover de nó**

A página Planejamento de failover de nó/desempenho estima o impactos no desempenho em um nó se o nó de parceiro de alta disponibilidade (HA) do nó falhar. O Unified Manager baseia as estimativas no desempenho histórico dos nós no par de HA.

Estimar o impactos de desempenho de um failover ajuda você a Planejar nos seguintes cenários:

- Se um failover degradar consistentemente o desempenho estimado do nó de takeover para um nível inaceitável, você pode considerar tomar ações corretivas para reduzir o impacto no desempenho devido a um failover.
- Antes de iniciar um failover manual para executar tarefas de manutenção de hardware, você pode estimar como o failover afeta o desempenho do nó de aquisição, a fim de determinar o melhor momento para executar a tarefa.

## **Usando a página Planejamento de failover de nó para determinar ações corretivas**

Com base nas informações exibidas na página Planejamento de failover de desempenho/nó, você pode tomar medidas para garantir que um failover não faça com que o desempenho de um par de HA caia abaixo de um nível aceitável.

Por exemplo, para reduzir o impacto estimado de um failover na performance, é possível mover alguns volumes ou LUNs de um nó no par de HA para outros nós no cluster. Fazer isso garante que o nó principal possa continuar a fornecer desempenho aceitável após um failover.

## **Componentes da página de Planejamento de failover de nó**

Os componentes da página Planejamento de failover de desempenho/nó são exibidos em uma grade e no painel de comparação. Essas seções permitem avaliar o impacto de um failover de nó na performance do nó de takeover.

## Grade de estatísticas de desempenho

A página Planejamento de failover de desempenho/nó exibe uma grade contendo estatísticas de latência, IOPS, utilização e capacidade de desempenho usada.



Os valores de latência e IOPS exibidos nesta página e na página Performance/Node Performance Explorer podem não corresponder porque diferentes contadores de desempenho são usados para calcular os valores para prever o failover do nó.

Na grade, cada nó recebe uma das seguintes funções:

- Primário

O nó que assume o parceiro de HA quando o parceiro falha. O objeto raiz é sempre o nó primário.

- Parceiro

O nó que falha no cenário de failover.

- Aquisição estimada

O mesmo que o nó principal. As estatísticas de desempenho exibidas para esse nó mostram o desempenho do nó de aquisição após assumir o parceiro com falha.



Embora a carga de trabalho do nó de takeover seja equivalente às cargas de trabalho combinadas de ambos os nós após um failover, as estatísticas do nó de takeover estimado não são a soma das estatísticas do nó principal e do nó do parceiro. Por exemplo, se a latência do nó principal for de 2 ms/op e a latência do nó Parceiro for de 3 ms/op, o nó de aquisição estimado poderá ter uma latência de 4 ms/op. Esse valor é um cálculo executado pelo Unified Manager.

Você pode clicar no nome do nó Parceiro se quiser que ele se torne o objeto raiz. Depois que a página Performance/Node Performance Explorer for exibida, você pode clicar na guia **Planejamento de failover** para ver como o desempenho muda neste cenário de falha de nó. Por exemplo, se Node1 for o nó principal e Node2 for o nó Parceiro, você poderá clicar em Node2 para torná-lo o nó principal. Dessa forma, você pode ver como o desempenho estimado muda dependendo de qual nó falhar.

## Painel de comparação

A lista a seguir descreve os componentes exibidos no painel de comparação por padrão:

- **Gráficos de eventos**

Eles são exibidos no mesmo formato que os da página Performance/Node Performance Explorer. Eles dizem respeito apenas ao nó primário.

- **Contador de gráficos**

Eles exibem estatísticas históricas para o contador de desempenho mostrado na grade. Em cada gráfico, o gráfico do nó de aquisição estimado mostra o desempenho estimado se um failover ocorreu em um determinado momento.

Por exemplo, suponha que o gráfico de utilização mostre 73% para o nó de aquisição estimado às 11 da manhã do dia 8 de fevereiro. Se um failover tivesse ocorrido naquele momento, a utilização do nó de

aquisição seria de 73%.

As estatísticas históricas ajudam você a encontrar o momento ideal para iniciar um failover, minimizando a possibilidade de sobrecarregar o nó de aquisição. Você pode agendar um failover apenas em momentos em que o desempenho previsto do nó de takeover seja aceitável.

Por padrão, as estatísticas do objeto raiz e do nó do parceiro são exibidas no painel de comparação. Ao contrário da página Performance/Node Performance Explorer, esta página não exibe o botão **Add** para adicionar objetos para comparação de estatísticas.

Você pode personalizar o painel de comparação da mesma maneira que faz na página Performance/Node Performance Explorer. A lista a seguir mostra exemplos de personalização dos gráficos:

- Clique no nome de um nó para mostrar ou ocultar as estatísticas do nó nos gráficos do contador.
- Clique em **Zoom View** para exibir um gráfico detalhado para um contador específico em uma nova janela.

## Usando uma política de limite com a página Planejamento de failover de nó

Você pode criar uma política de limite de nó para que você possa ser notificado na página Planejamento de failover de nó/desempenho quando um potencial failover degradar o desempenho do nó de aquisição para um nível inaceitável.

A política de limite de desempenho definido pelo sistema denominada ""par de HA de nós sobreutilizado"" gera um evento de aviso se o limite for violado por seis períodos de coleta consecutivos (30 minutos). O limite é considerado violado se a capacidade de performance combinada usada pelos nós em um par de HA exceder 200%.

O evento da política de limite definido pelo sistema alerta você para o fato de que um failover fará com que a latência do nó de takeover aumente para um nível inaceitável. Quando você vê um evento gerado por essa diretiva para um nó específico, você pode navegar para a página Planejamento de failover de Performance/nó para esse nó para exibir o valor de latência previsto devido a um failover.

Além de usar essa política de limite definida pelo sistema, você pode criar políticas de limite usando o contador "capacidade de desempenho usada - aquisição" e, em seguida, aplicar a política aos nós selecionados. Especificar um limite inferior a 200% permite que você receba um evento antes que o limite para a política definida pelo sistema seja violado. Você também pode especificar o período mínimo de tempo para o qual o limite é excedido para menos de 30 minutos se quiser ser notificado antes que o evento de política definido pelo sistema seja gerado.

Por exemplo, você pode definir uma política de limite para gerar um evento de aviso se a capacidade combinada de performance usada pelos nós em um par de HA exceder 175% por mais de 10 minutos. Você pode aplicar essa política ao Node1 e ao Node2, que formam um par de HA. Depois de receber uma notificação de evento de aviso para Node1 ou Node2, você pode visualizar a página Planejamento de failover de nó/desempenho para esse nó para avaliar o impacto estimado no desempenho no nó de aquisição. Você pode tomar medidas corretivas para evitar sobrecarregar o nó de takeover se ocorrer um failover. Se você agir quando a capacidade combinada de performance usada pelos nós for inferior a 200%, a latência do nó de takeover não atinge um nível inaceitável mesmo que um failover ocorra durante esse período.

## Uso do gráfico de repartição capacidade de desempenho usado para Planejamento de failover

O gráfico detalhado de capacidade de desempenho usada - detalhamento mostra a

capacidade de desempenho usada para o nó principal e o nó do parceiro. Ele também mostra a quantidade de capacidade de desempenho livre no nó de takeover estimado. Essas informações ajudam a determinar se você pode ter um problema de desempenho se o nó do parceiro falhar.

Além de mostrar a capacidade total de desempenho usada para os nós, o gráfico de repartição divide os valores de cada nó em protocolos de usuário e processos em segundo plano.

- Os protocolos de usuário são as operações de e/S de aplicativos de usuário de e para o cluster.
- Processos em segundo plano são os processos internos do sistema envolvidos com eficiência de storage, replicação de dados e integridade do sistema.

Esse nível adicional de detalhes permite determinar se um problema de desempenho é causado pela atividade do aplicativo do usuário ou pelos processos do sistema em segundo plano, como deduplicação, reconstrução RAID, análise de disco e cópias SnapMirror.

### Passos

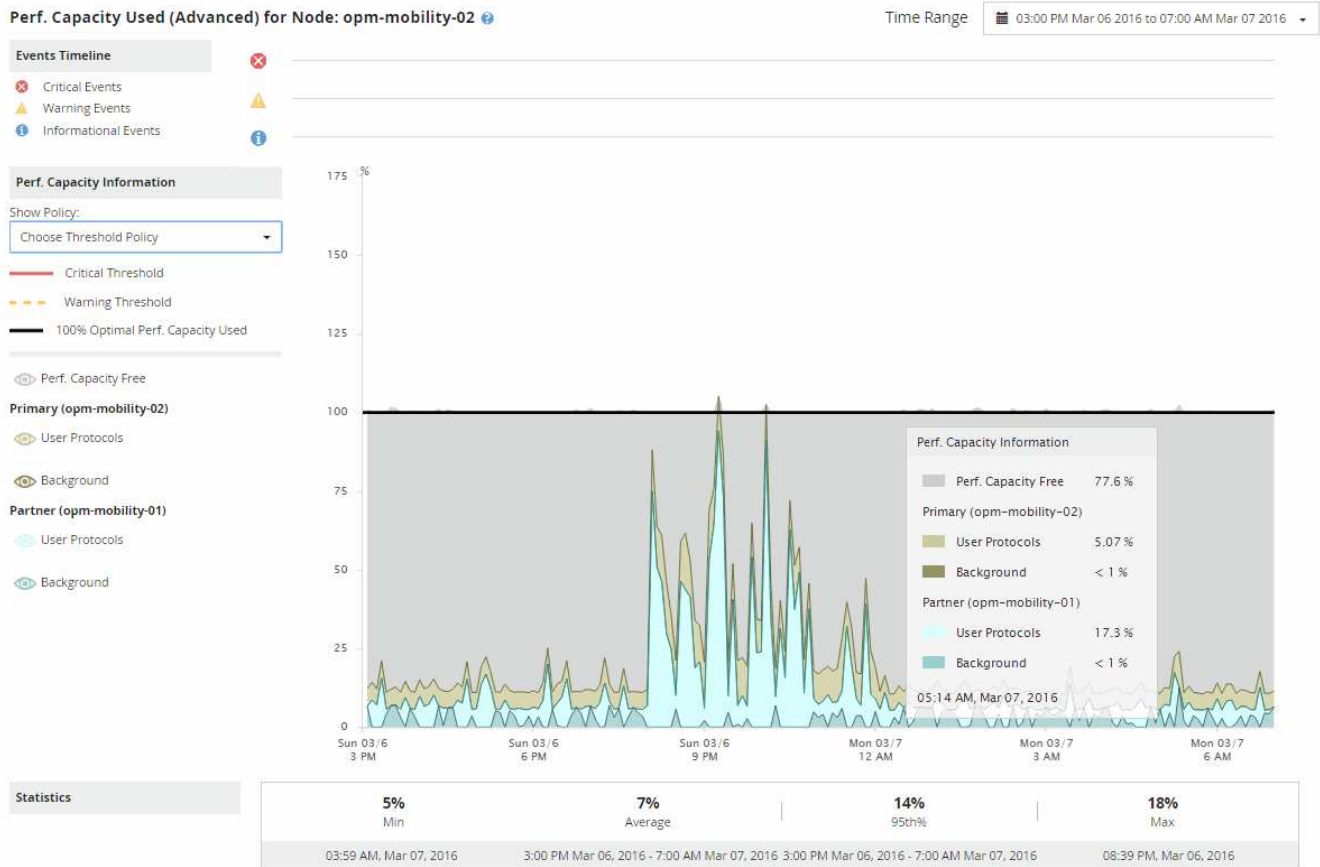
1. Vá para a página **Planejamento de failover de desempenho/nó** para o nó que servirá como o nó de aquisição estimado.
2. No seletor **intervalo de tempo**, escolha o período de tempo para o qual as estatísticas históricas são exibidas na grade do contador e nos gráficos do contador.

Os gráficos de contador com estatísticas para o nó principal, nó do parceiro e nó de aquisição estimado são exibidos.

3. Na lista **escolha gráficos**, selecione **Perf. Capacidade utilizada**.
4. No **Perf. Capacidade usada** gráfico, selecione **Breakdown** e clique em **Zoom View**.

O gráfico detalhado para Perf. A capacidade utilizada é apresentada.





5. Mova o cursor sobre o gráfico detalhado para ver as informações de capacidade de desempenho usadas na janela pop-up.

O Perf. A porcentagem de livre de capacidade é a capacidade de desempenho disponível no nó de aquisição estimado. Ele indica quanto de capacidade de desempenho é deixada no nó de takeover após um failover. Se for 0%, um failover fará com que a latência aumente para um nível inaceitável no nó de takeover.

6. Considere tomar ações corretivas para evitar uma porcentagem livre de capacidade de baixo desempenho.

Se você pretende iniciar um failover para manutenção de nós, escolha um momento para falhar no nó do parceiro quando a porcentagem de disponibilidade de capacidade de performance não for de 0.

## Coleta de dados e monitoramento do desempenho da carga de trabalho

O Unified Manager coleta e analisa a atividade do workload a cada 5 minutos para identificar eventos de performance e detecta alterações de configuração a cada 15 minutos. Ele retém um máximo de 30 dias de dados de eventos e performance históricos de 5 minutos e usa esses dados para prever o intervalo de latência esperado para todos os workloads monitorados.

O Unified Manager deve coletar no mínimo 3 dias de atividade do workload antes que ele possa começar a análise e antes que a previsão de latência do tempo de resposta de e/S possa ser exibida na página análise

do workload e na página de detalhes do evento. Enquanto essa atividade está sendo coletada, a previsão de latência não exibe todas as alterações que ocorrem na atividade da carga de trabalho. Após coletar 3 dias de atividade, o Unified Manager ajusta a previsão de latência a cada 24 horas às 12:00 da manhã, para refletir as alterações nas atividades do workload e estabelecer um limite de performance dinâmico mais preciso.

Durante os primeiros 4 dias em que o Unified Manager está monitorando uma carga de trabalho, se mais de 24 horas passaram desde a última coleta de dados, os gráficos de latência não exibirão a previsão de latência para essa carga de trabalho. Os eventos detetados antes da última coleção ainda estão disponíveis.



O horário de verão (DST) altera a hora do sistema, o que altera a previsão de latência das estatísticas de desempenho para cargas de trabalho monitoradas. O Unified Manager começa imediatamente a corrigir a previsão de latência, que leva aproximadamente 15 dias para ser concluída. Durante esse período, você pode continuar usando o Unified Manager, mas, como o Unified Manager usa a previsão de latência para detetar eventos dinâmicos, alguns eventos podem não ser precisos. Os eventos detetados antes da alteração de hora não são afetados.

## Tipos de workloads monitorados pelo Unified Manager

Você pode usar o Unified Manager para monitorar a performance de dois tipos de workloads: Definido pelo usuário e definido pelo sistema.

### • *cargas de trabalho definidas pelo usuário*

A taxa de transferência de e/S das aplicações para o cluster. Estes são processos envolvidos em pedidos de leitura e escrita. Um volume, LUN, compartilhamento NFS, compartilhamento SMB/CIFS e um workload são um workload definido pelo usuário.



O Unified Manager monitora apenas a atividade do workload no cluster. Ele não monitora os aplicativos, os clientes ou os caminhos entre os aplicativos e o cluster.

Se uma ou mais das opções a seguir for verdadeira para uma carga de trabalho, ela não poderá ser monitorada pelo Unified Manager:

- É uma cópia de proteção de dados (DP) no modo somente leitura. (Os volumes DP são monitorados quanto ao tráfego gerado pelo usuário.)
- É um clone de dados off-line.
- É um volume espelhado em uma configuração do MetroCluster.

### • *cargas de trabalho definidas pelo sistema*

Os processos internos envolvidos com eficiência de storage, replicação de dados e integridade do sistema, incluindo:

- Eficiência de storage, como deduplicação
- Integridade do disco, que inclui RAID Reconstruct, análise de disco e assim por diante
- Replicação de dados, como cópias SnapMirror
- Atividades de gestão
- Integridade do sistema de arquivos, que inclui várias atividades do WAFL
- Scanners de sistema de arquivos, como WAFL scan
- Descarga de cópia, como operações de eficiência de storage descarregadas de hosts VMware

- Integridade do sistema, como movimentos de volume, compactação de dados etc.
- Volumes não monitorizados

Os dados de performance para workloads definidos pelo sistema são exibidos na GUI somente quando o componente de cluster usado por esses workloads está na contenção. Por exemplo, você não pode pesquisar o nome de uma carga de trabalho definida pelo sistema para exibir seus dados de performance na GUI.



## Valores de medição de performance de workload

O Unified Manager mede o desempenho de workloads em um cluster com base em valores estatísticos históricos e esperados, que formam a previsão de latência de valores para as cargas de trabalho. Ele compara os valores estatísticos reais de workload com a previsão de latência para determinar quando a performance do workload é muito alta ou muito baixa. Uma carga de trabalho que não está funcionando como esperado aciona um evento de desempenho dinâmico para notificá-lo.

Na ilustração a seguir, o valor real, em vermelho, representa as estatísticas reais de desempenho no período de tempo. O valor real cruzou o limite de desempenho, que é os limites superiores da previsão de latência. O pico é o valor real mais alto no período de tempo. O desvio mede a mudança entre os valores esperados (a previsão) e os valores reais, enquanto o desvio de pico indica a maior mudança entre os valores esperados e os valores reais.



A tabela a seguir lista os valores de medição de desempenho da carga de trabalho.

Medição	Descrição
Atividade	<p>Porcentagem do limite de QoS usado pelos workloads no grupo de políticas.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>Se o Unified Manager detetar uma alteração em um grupo de políticas, como adicionar ou remover um volume ou alterar o limite de QoS, os valores real e esperado poderão exceder 100% do limite definido. Se um valor exceder 100% do limite definido, é apresentado como &gt;100%. Se um valor for inferior a 1% do limite definido, é apresentado como inferior a 1%.</p> </div>
Real	O valor de desempenho medido em um momento específico para uma determinada carga de trabalho.
Desvio	<p>A mudança entre os valores esperados e os valores reais. É a relação do valor real menos o valor esperado para o valor superior do intervalo esperado menos o valor esperado.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>Um valor de desvio negativo indica que o desempenho da carga de trabalho é inferior ao esperado, enquanto um valor de desvio positivo indica que o desempenho da carga de trabalho é superior ao esperado.</p> </div>
Esperado	Os valores esperados são baseados na análise de dados históricos de performance para uma determinada carga de trabalho. O Unified Manager analisa esses valores estatísticos para determinar o intervalo esperado (previsão de latência) dos valores.
Previsão de latência (intervalo esperado)	A previsão de latência é uma previsão do que os valores de desempenho superior e inferior devem ser em um momento específico. Para a latência do workload, os valores superiores formam o limite de performance. Quando o valor real cruza o limite de performance, o Unified Manager aciona um evento de performance dinâmico.
Pico	O valor máximo medido durante um período de tempo.

<b>Medição</b>	<b>Descrição</b>
Desvio máximo	O valor de desvio máximo medido durante um período de tempo.
Profundidade da fila	O número de solicitações de e/S pendentes que estão aguardando no componente de interconexão.
Utilização	Para os componentes de processamento de rede, Data Processing e agregado, a porcentagem de tempo de ocupado para concluir as operações de carga de trabalho por um período de tempo. Por exemplo, a porcentagem de tempo para o processamento de rede ou os componentes do Data Processing processarem uma solicitação de e/S ou para um agregado atender a uma solicitação de leitura ou gravação.
Taxa de transferência de gravação	A quantidade de taxa de transferência de gravação, em megabytes por segundo (MB/s), desde cargas de trabalho em um cluster local até o cluster de parceiros em uma configuração do MetroCluster.

## **Qual é a faixa de desempenho esperada**

A previsão de latência é uma previsão do que os valores de desempenho superior e inferior devem ser em um momento específico. Para a latência do workload, os valores superiores formam o limite de performance. Quando o valor real cruza o limite de performance, o Unified Manager aciona um evento de performance dinâmico.

Por exemplo, durante o horário comercial regular entre as 9:00h e as 5:00h, a maioria dos funcionários pode verificar seu e-mail entre as 9:00h e as 10:30H. o aumento da demanda nos servidores de e-mail significa um aumento na atividade de carga de trabalho no armazenamento de back-end durante esse período. Os funcionários podem notar um tempo de resposta lento de seus clientes de e-mail.

Durante a hora de almoço entre as 12:00h e as 1:00h e no final do dia de trabalho após as 5:00h, a maioria dos funcionários provavelmente está longe de seus computadores. A demanda nos servidores de e-mail geralmente diminui, também diminuindo a demanda no armazenamento de back-end. Como alternativa, pode haver operações de carga de trabalho agendadas, como backups de armazenamento ou verificação de vírus, que começam após as 5:00 horas e aumentam a atividade no armazenamento de back-end.

Ao longo de vários dias, o aumento e a diminuição da atividade de workload determinam o intervalo esperado (previsão de latência) da atividade, com limites superior e inferior para uma carga de trabalho. Quando a atividade de carga de trabalho real para um objeto está fora dos limites superior ou inferior e permanece fora dos limites por um período de tempo, isso pode indicar que o objeto está sendo usado em excesso ou subutilizado.

## **Como a previsão de latência é formada**

O Unified Manager deve coletar no mínimo 3 dias de atividade do workload antes que ele possa iniciar a análise e antes que a previsão de latência do tempo de resposta de e/S possa ser exibida na GUI. A coleta de

dados mínima necessária não é responsável por todas as alterações que ocorrem na atividade da carga de trabalho. Após coletar os primeiros 3 dias de atividade, o Unified Manager ajusta a previsão de latência a cada 24 horas às 12:00 da manhã para refletir as alterações na atividade do workload e estabelecer um limite de performance dinâmico mais preciso.



O horário de verão (DST) altera a hora do sistema, o que altera a previsão de latência das estatísticas de desempenho para cargas de trabalho monitoradas. O Unified Manager começa imediatamente a corrigir a previsão de latência, que leva aproximadamente 15 dias para ser concluída. Durante esse período, você pode continuar usando o Unified Manager, mas, como o Unified Manager usa a previsão de latência para detectar eventos dinâmicos, alguns eventos podem não ser precisos. Os eventos detectados antes da alteração de hora não são afetados.

## Como a previsão de latência é usada na análise de desempenho

O Unified Manager usa a previsão de latência para representar a atividade típica de latência de e/S (tempo de resposta) dos workloads monitorados. Ele alerta quando a latência real de um workload está acima dos limites superiores da previsão de latência, que aciona um evento de performance dinâmico, para que você possa analisar o problema de performance e tomar medidas corretivas para resolvê-lo.

A previsão de latência define a linha de base de desempenho para a carga de trabalho. Com o tempo, o Unified Manager aprende com medições de desempenho anteriores para prever os níveis de desempenho e atividade esperados para a carga de trabalho. O limite superior do intervalo esperado estabelece o limite de desempenho dinâmico. O Unified Manager usa a linha de base para determinar quando a latência real está acima ou abaixo de um limite ou fora dos limites de seu intervalo esperado. A comparação entre os valores reais e os valores esperados cria um perfil de performance para a carga de trabalho.

Quando a latência real de um workload excede o limite dinâmico de performance, devido à contenção em um componente do cluster, a latência é alta e o workload opera mais lentamente do que o esperado. O desempenho de outras cargas de trabalho que compartilham os mesmos componentes de cluster também pode ser mais lento do que o esperado.

O Unified Manager analisa o evento de cruzamento de limites e determina se a atividade é um evento de desempenho. Se a atividade de alto workload permanecer consistente por um longo período de tempo, como várias horas, o Unified Manager considera a atividade normal e ajusta dinamicamente a previsão de latência para formar o novo limite dinâmico de performance.

Algumas cargas de trabalho podem ter atividades consistentemente baixas, em que a previsão de latência para latência não tem uma alta taxa de alteração ao longo do tempo. Para minimizar o número de eventos durante a análise de eventos de performance, o Unified Manager aciona um evento apenas para volumes de baixa atividade cujas operações e latências são muito maiores do que o esperado.



Neste exemplo, a latência de um volume tem uma previsão de latência, em cinza, de 3,5 milissegundos por operação (ms/op) no menor e 5,5 ms/op no máximo. Se a latência real, em azul, aumentar repentinamente para 10 ms/op, devido a um pico intermitente no tráfego de rede ou contenção em um componente de cluster, ela fica então acima da previsão de latência e excede o limite de desempenho dinâmico.

Quando o tráfego de rede diminuiu ou o componente do cluster não está mais na contenção, a latência retorna dentro da previsão de latência. Se a latência permanecer em ou acima de 10 ms/op por um longo período de tempo, talvez seja necessário tomar medidas corretivas para resolver o evento.

## Como o Unified Manager usa a latência do workload para identificar problemas de performance

A latência do workload (tempo de resposta) é o tempo necessário para um volume em um cluster responder a solicitações de e/S de aplicativos clientes. O Unified Manager usa a latência para detectar e alertar você sobre eventos de performance.

Uma alta latência significa que as solicitações de aplicativos para um volume em um cluster estão demorando mais do que o normal. A causa da alta latência pode estar no próprio cluster, devido à contenção em um ou mais componentes do cluster. A alta latência também pode ser causada por problemas fora do cluster, como gargalos de rede, problemas com o cliente que hospeda os aplicativos ou problemas com os próprios aplicativos.

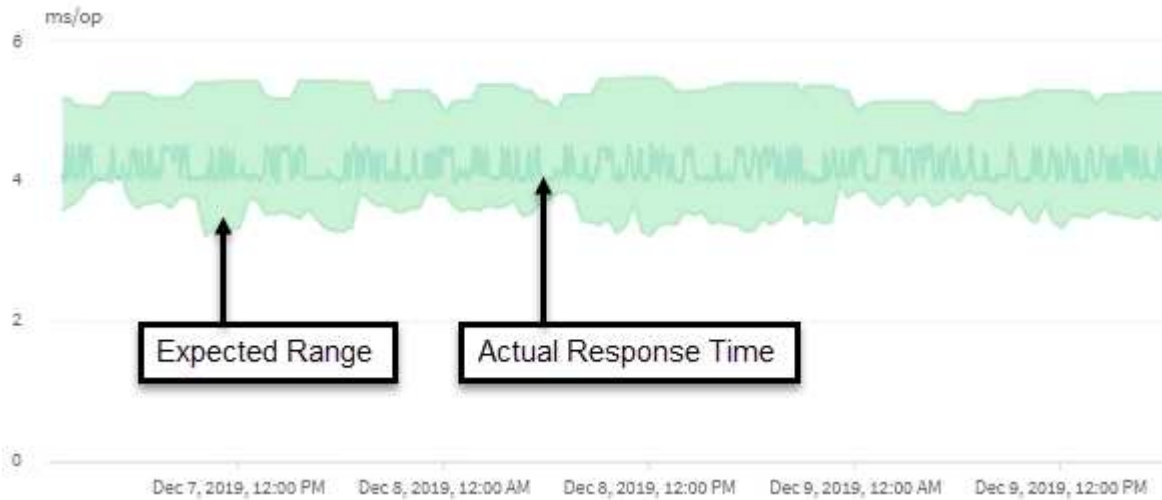


O Unified Manager monitora apenas a atividade do workload no cluster. Ele não monitora os aplicativos, os clientes ou os caminhos entre os aplicativos e o cluster.

As operações no cluster, como fazer backups ou executar deduplicação, que aumentam a demanda por componentes de cluster compartilhados por outros workloads, também podem contribuir para a alta latência. Se a latência real exceder o limite de desempenho dinâmico do intervalo esperado (previsão de latência), o Unified Manager analisa o evento para determinar se é um evento de desempenho que talvez você precise resolver. A latência é medida em milissegundos por operação (ms/op).

No gráfico total de latência na página análise de workload, é possível visualizar uma análise das estatísticas de latência para ver como a atividade de processos individuais, como solicitações de leitura e gravação, se compara às estatísticas de latência geral. A comparação ajuda você a determinar quais operações têm a atividade mais alta ou se operações específicas têm atividade anormal que está afetando a latência de um volume. Ao analisar eventos de desempenho, você pode usar as estatísticas de latência para determinar se um evento foi causado por um problema no cluster. Você também pode identificar as atividades específicas de

workload ou os componentes de cluster envolvidos no evento.



Este exemplo mostra o gráfico de latência. A atividade de tempo de resposta real (latência) é uma linha azul e a previsão de latência (intervalo esperado) é verde.

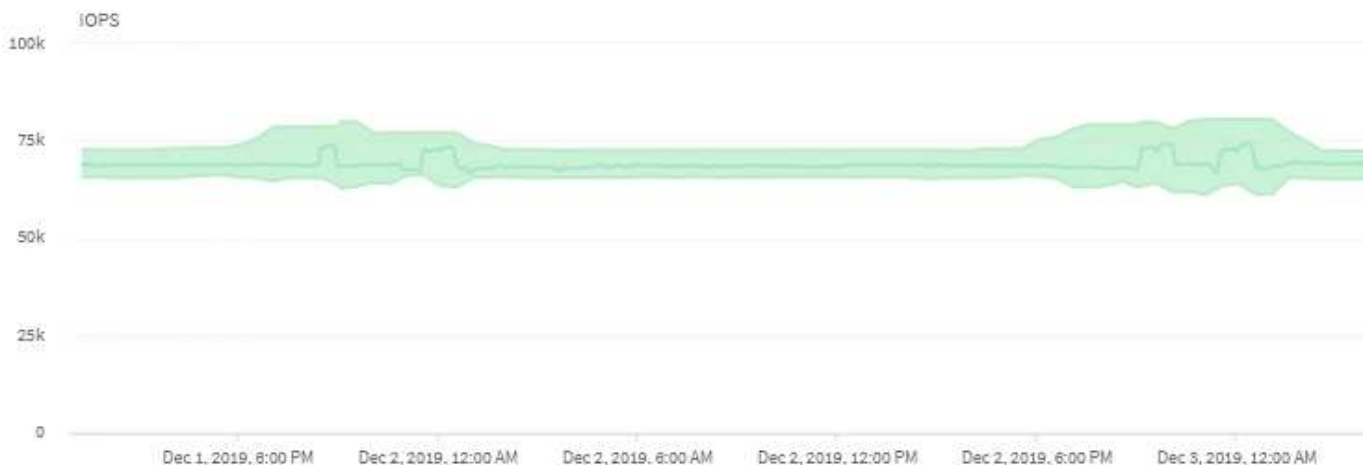


Pode haver lacunas na linha azul se o Unified Manager não conseguir coletar dados. Isso pode ocorrer porque o cluster ou o volume estava inalcançável, o Unified Manager foi desativado durante esse tempo ou a coleção demorava mais do que o período de coleta de 5 minutos.

## Como as operações do cluster podem afetar a latência do workload

As operações (IOPS) representam a atividade de todos os workloads definidos pelo usuário e definidos pelo sistema em um cluster. As estatísticas de IOPS ajudam a determinar se os processos de cluster, como fazer backups ou executar deduplicação, estão impactando a latência do workload (tempo de resposta) ou podem ter causado ou contribuído para um evento de performance.

Ao analisar eventos de desempenho, você pode usar as estatísticas de IOPS para determinar se um evento de desempenho foi causado por um problema no cluster. Você pode identificar as atividades específicas de carga de trabalho que podem ter sido os principais contribuintes para o evento de performance. As operações de entrada/saída por segundo (operações/seg) são medidas em operações por segundo (operações/seg).





Este exemplo mostra o gráfico de IOPS. As estatísticas de operações reais são uma linha azul e a previsão de operações de IOPS é verde.



Em alguns casos em que um cluster está sobrecarregado, o Unified Manager pode exibir a mensagem `Data collection is taking too long on Cluster cluster_name`. Isso significa que não foram coletadas estatísticas suficientes para que o Unified Manager analise. Você precisa reduzir os recursos que o cluster está usando para que as estatísticas possam ser coletadas.

## Monitoramento de desempenho das configurações do MetroCluster

Com o Unified Manager, você monitora a taxa de transferência de gravação entre clusters em uma configuração do MetroCluster para identificar workloads com uma taxa de transferência de gravação alta.

Se esses workloads de alta performance fizerem com que outros volumes no cluster local tenham tempos de resposta de e/S altos, o Unified Manager acionará eventos de desempenho para notificá-lo.



O Unified Manager trata os clusters em uma configuração do MetroCluster como clusters individuais. Isso não faz distinção entre clusters que são parceiros ou correlacionam a taxa de transferência de gravação de cada cluster.

Quando um cluster local em uma configuração do MetroCluster espelha seus dados em seu cluster de parceiros, os dados são gravados no NVRAM e transferidos pelos links de interswitch (ISLs) para os agregados remotos. O Unified Manager analisa o NVRAM para identificar workloads cuja alta taxa de transferência de gravação sobreutiliza o NVRAM, colocando o NVRAM na contenção.

Cargas de trabalho cujo desvio no tempo de resposta excedeu o limite de desempenho são chamadas *vítimas* e cargas de trabalho cujo desvio no throughput de gravação para o NVRAM é maior do que o habitual, causando a contenção, são chamadas *bullies*. Como apenas as solicitações de gravação são espelhadas no cluster de parceiros, o Unified Manager não analisa a taxa de transferência de leitura.

É possível visualizar a taxa de transferência de qualquer um dos clusters em uma configuração do MetroCluster analisando os workloads das LUNs e volumes correspondentes nas telas a seguir. Você pode filtrar os resultados pelo cluster. A partir do painel de navegação esquerdo:

- **Storage > clusters > desempenho: Exibição todos os clusters.** Consulte
- **Armazenamento > volumes > desempenho: Visualização de todos os volumes.**
- **Armazenamento > LUNs > desempenho: Todos os LUNs** são exibidos.
- **Análise de cargas de trabalho > todas as cargas de trabalho**

### Informações relacionadas

["Análise e notificação de eventos de performance"](#)

["Análise de eventos de performance para uma configuração do MetroCluster"](#)

["Funções dos workloads envolvidos em um evento de desempenho"](#)

["Identificação das cargas de trabalho das vítimas envolvidas em um evento de desempenho"](#)

["Identificação de cargas de trabalho bully envolvidas em um evento de desempenho"](#)

## Compreender eventos e alertas de desempenho

Os eventos de desempenho são incidentes relacionados ao desempenho da carga de trabalho em um cluster. Eles ajudam a identificar workloads com tempos de resposta lentos. Juntamente com 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.

Quando o Unified Manager detecta várias ocorrências da mesma condição de evento para o mesmo componente de cluster, ele trata todas as ocorrências como um único evento, não como eventos separados.

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 sobrecarregam 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 as cargas de trabalho em um sistema ONTAP estão lentas devido a outras cargas de trabalho 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 detecta uma alteração de configuração.

Para obter mais informações, consulte os seguintes links:

- ["O que acontece quando um evento é recebido"](#)
- ["Quais informações estão contidas em um e-mail de alerta"](#)
- ["Adicionar alertas"](#)
- ["Adição de alertas para eventos de desempenho"](#)

## 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 análise de carga de trabalho para ver se o evento de mudança 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 (MB/s 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.

## 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 você estiver recebendo eventos desnecessários de qualquer política de limite de desempenho definido pelo sistema, poderá desativar os eventos para políticas individuais na página Configuração de eventos.

### Políticas de limite de cluster

As políticas de limite de performance do cluster definido pelo sistema são atribuídas, por padrão, a cada cluster monitorado pelo Unified Manager:

- \* Desequilíbrio de carga de cluster\*

Identifica situações em que um nó está operando com uma carga muito maior do que outros nós no cluster e, portanto, potencialmente afetando as latências de workload.

Ele faz isso comparando o valor da capacidade de performance usada para todos os nós em um cluster para ver se algum nó excedeu o valor do limite de 30% por mais de 24 horas. Este é um evento de aviso.

- **Desequilíbrio da capacidade do cluster**

Identifica situações em que um agregado tem uma capacidade usada muito maior do que outros agregados no cluster e, portanto, potencialmente afetando o espaço necessário para as operações.

Ele faz isso comparando o valor de capacidade usado para todos os agregados no cluster para ver se há uma diferença de 70% entre todos os agregados. Este é um evento de aviso.

## **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:

- **Limite de capacidade de desempenho usado violado**

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

Para isso, é necessário procurar nós que estejam usando mais de 100% da capacidade de performance por mais de 12 horas. Este é um evento de aviso.

- **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.

Para isso, observe o valor da capacidade de performance usada para os dois nós do par de HA. Se a capacidade de performance combinada usada nos dois nós exceder 200% por mais de 12 horas, um failover de controladora afetará as latências de workload. Este é um evento informativo.

- **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 resincronização 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 cada agregado 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 resincronização 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 latência do workload

As políticas de limite de latência de workload definidas pelo sistema são atribuídas a qualquer workload que tenha uma política de nível de Serviço de Performance configurada que tenha um valor definido de "latência esperada":

- **Limite de latência de volume/LUN de carga de trabalho violado conforme definido pelo nível de Serviço de Performance**

Identifica volumes (compartilhamentos de arquivos) e LUNs que excederam o limite de latência esperada, e que estão afetando a performance do workload. Este é um evento de aviso.

Isso ocorre procurando cargas de trabalho que excederam o valor de latência esperado por 30% do tempo na hora anterior.

### 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 MB/s). 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 MB/s de QoS**

Identifica volumes e LUNs que excederam o limite máximo de IOPS ou taxa de transferência MB/s 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 MB/s 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 máximo de MB/s de QoS com base no tamanho de cada volume. Em seguida, ele procura volumes que excederam o QoS máximo MB/s 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.

## Análise e notificação de eventos de performance

Os eventos de desempenho notificam você sobre problemas de desempenho de e/S em uma carga de trabalho causada pela contenção em um componente do cluster. O Unified Manager analisa o evento para identificar todos os workloads envolvidos, o componente em contenção e se o evento ainda é um problema que talvez você precise resolver.

O Unified Manager monitora a latência de e/S (tempo de resposta) e IOPS (operações) de volumes em um cluster. Quando outras cargas de trabalho usam excessivamente um componente de cluster, por exemplo, o componente está na contenção e não pode ter desempenho em um nível ideal para atender às demandas de workload. O desempenho de outros workloads que estão usando o mesmo componente pode ser afetado, causando o aumento de suas latências. Se a latência ultrapassar o limite de desempenho dinâmico, o Unified Manager acionará um evento de desempenho para notificá-lo.

### Análise de eventos

O Unified Manager realiza as seguintes análises, usando as estatísticas de desempenho dos 15 dias anteriores, para identificar os workloads da vítima, os workloads bully e o componente do cluster envolvido em um evento:

- Identifica cargas de trabalho da vítima cuja latência ultrapassou o limite de desempenho dinâmico, que é o limite superior da previsão de latência:
  - Para volumes em agregados híbridos HDD ou Flash Pool (camada local), os eventos são acionados somente quando a latência é maior que 5 milissegundos (ms) e o IOPS é mais de 10 operações por segundo (operações/seg).
  - Para volumes em agregados all-SSD ou agregados FabricPool (camada de nuvem), os eventos são acionados apenas quando a latência é superior a 1 ms e o IOPS é superior a 100 operações/seg
- Identifica o componente do cluster na contenção.



Se a latência das cargas de trabalho da vítima na interconexão de cluster for superior a 1 ms, o Unified Manager tratará isso como significativo e acionará um evento para a interconexão de cluster.

- Identifica as cargas de trabalho bully que estão sobreusando o componente do cluster e fazendo com que ele esteja na contenção.

- Classifica as cargas de trabalho envolvidas, com base em seu desvio na utilização ou atividade de um componente de cluster, para determinar quais bullies têm a maior alteração no uso do componente de cluster e quais vítimas são as mais impactadas.

Um evento pode ocorrer por apenas um breve momento e depois se corrigir depois que o componente que está usando não está mais em disputa. Um evento contínuo é aquele que ocorre novamente para o mesmo componente do cluster dentro de um intervalo de cinco minutos e permanece no estado ativo. Para eventos contínuos, o Unified Manager aciona um alerta após detectar o mesmo evento durante dois intervalos de análise consecutivos.

Quando um evento é resolvido, ele permanece disponível no Unified Manager como parte do Registro de problemas de desempenho anteriores de um volume. Cada evento tem um ID exclusivo que identifica o tipo de evento e os volumes, o cluster e os componentes do cluster envolvidos.



Um único volume pode ser envolvido em mais de um evento ao mesmo tempo.

## Estado do evento

Os eventos podem estar em um dos seguintes estados:

- **Ativo**

Indica que o evento de desempenho está ativo no momento (novo ou confirmado). O problema que causa o evento não foi corrigido ou não foi resolvido. O contador de performance do objeto de storage permanece acima do limite de performance.

- **Obsoleto**

Indica que o evento já não está ativo. O problema que causa o evento foi corrigido ou foi resolvido. O contador de desempenho do objeto de storage não está mais acima do limite de desempenho.

## Notificação de evento

Os eventos são exibidos na página Painel e em muitas outras páginas na interface do usuário, e os alertas desses eventos são enviados para endereços de e-mail especificados. Você pode exibir informações de análise detalhadas sobre um evento e obter sugestões para resolvê-lo na página de detalhes do evento e na página análise de carga de trabalho.

## Interação de eventos

Na página Detalhes do evento e na página análise de carga de trabalho, você pode interagir com eventos das seguintes maneiras:

- Mover o Mouse sobre um evento exibe uma mensagem que mostra a data e a hora em que o evento foi detectado.

Se houver vários eventos para o mesmo período de tempo, a mensagem mostrará o número de eventos.

- Clicar em um único evento exibe uma caixa de diálogo que mostra informações mais detalhadas sobre o evento, incluindo os componentes do cluster envolvidos.

O componente em contenção é circulado e realçado a vermelho. Você pode clicar em **Exibir análise completa** para ver a análise completa na página de detalhes do evento. Se houver vários eventos para o mesmo período de tempo, a caixa de diálogo mostra detalhes sobre os três eventos mais recentes. Você



pode clicar em um evento para exibir a análise do evento na página de detalhes do evento.

## Como o Unified Manager determina o impacto no desempenho de um evento

O Unified Manager usa o desvio na atividade, utilização, taxa de transferência de gravação, uso de componentes do cluster ou latência de e/S (tempo de resposta) para um workload a fim de determinar o nível de impacto na performance do workload. Essas informações determinam a função de cada carga de trabalho no evento e como eles são classificados na página de detalhes do evento.

O Unified Manager compara os últimos valores analisados para uma carga de trabalho com o intervalo esperado (previsão de latência) de valores. A diferença entre os valores analisados pela última vez e o intervalo esperado de valores identifica as cargas de trabalho cujo desempenho foi mais impactado pelo evento.

Por exemplo, suponha que um cluster contenha duas cargas de trabalho: Carga de Trabalho A e carga de trabalho B. a previsão de latência para carga de trabalho A é de 5-10 milissegundos por operação (ms/op) e sua latência real geralmente é de cerca de 7 ms/op. A previsão de latência para o workload B é de 10-20 ms/op e sua latência real geralmente é de cerca de 15 ms/op. Ambos os workloads estão bem dentro da previsão de latência. Devido à contenção no cluster, a latência de ambas as cargas de trabalho aumenta para 40 ms/op, cruzando o limite de desempenho dinâmico, que é os limites superiores da previsão de latência e acionando eventos. O desvio de latência, dos valores esperados para os valores acima do limite de desempenho, para a carga de trabalho A é de cerca de 33 ms/op, e o desvio para carga de trabalho B é de cerca de 25 ms/op. A latência de ambas as cargas de trabalho aumenta para 40 ms/op, mas o Workload A teve maior impacto no desempenho, pois teve maior desvio de latência em 33 ms/op.

Na página de detalhes do evento, na seção Diagnóstico do sistema, você pode classificar as cargas de trabalho por seu desvio na atividade, utilização ou taxa de transferência de um componente do cluster. Você também pode classificar workloads por latência. Quando você seleciona uma opção de classificação, o Unified Manager analisa o desvio na atividade, utilização, taxa de transferência ou latência desde que o evento foi detectado a partir dos valores esperados para determinar a ordem de classificação da carga de trabalho. Para a latência, os pontos vermelhos (●) indicam um cruzamento de limite de desempenho por uma carga de trabalho da vítima e o impactos subsequente na latência. Cada ponto vermelho indica um nível mais alto de desvio na latência, o que ajuda a identificar as cargas de trabalho da vítima cuja latência foi mais afetada por um evento.

## Componentes do cluster e por que eles podem estar na contenção

Você pode identificar problemas de desempenho do cluster quando um componente do cluster entra em contenção. O desempenho de workloads que usam o componente diminui e seu tempo de resposta (latência) para solicitações do cliente aumenta, o que aciona um evento no Unified Manager.

Um componente que está em disputa não pode funcionar em um nível ideal. Seu desempenho diminuiu e o desempenho de outros componentes e cargas de trabalho do cluster, chamados *vítimas*, pode ter aumentado a latência. Para sair da contenção de um componente, você precisa reduzir o workload ou aumentar a capacidade de lidar com mais trabalho, para que a performance possa retornar aos níveis normais. Como o Unified Manager coleta e analisa a performance do workload em intervalos de cinco minutos, ele detecta quando um componente do cluster é consistentemente sobreutilizado. Não são detectados picos transitórios de sobreutilização que duram apenas uma curta duração dentro do intervalo de cinco minutos.

Por exemplo, um agregado de storage pode estar sob contenção porque um ou mais workloads nele estão

competindo para que suas solicitações de e/S sejam atendidas. Outras cargas de trabalho no agregado podem ser afetadas, fazendo com que seu desempenho diminua. Para reduzir a quantidade de atividade no agregado, há etapas diferentes, como mover uma ou mais workloads para um agregado ou nó menos ocupado, para diminuir a demanda geral de workload no agregado atual. Para um grupo de políticas de QoS, você pode ajustar o limite de taxa de transferência ou mover workloads para um grupo de políticas diferente, para que os workloads não fiquem mais sendo controlados.

O Unified Manager monitora os seguintes componentes do cluster para alertá-lo quando eles estão na contenção:

- **Rede**

Representa o tempo de espera das solicitações de e/S pelos protocolos de rede externos no cluster. O tempo de espera é o tempo gasto esperando que as transações "prontas para transferência" sejam concluídas antes que o cluster possa responder a uma solicitação de e/S. Se o componente de rede estiver em contenção, isso significa que o alto tempo de espera na camada de protocolo está impactando a latência de uma ou mais cargas de trabalho.

- **Processamento de rede**

Representa o componente de software no cluster envolvido com o processamento de e/S entre a camada de protocolo e o cluster. O processamento da rede de tratamento do nó pode ter sido alterado desde que o evento foi detectado. Se o componente de processamento de rede estiver em contenção, isso significa que a alta utilização no nó de processamento de rede está impactando a latência de uma ou mais cargas de trabalho.

Ao usar um cluster All SAN Array em uma configuração ativo-ativo, o valor de latência de processamento de rede é exibido para ambos os nós para que você possa verificar se os nós estão compartilhando a carga igualmente.

- **\* Limite de QoS Max\***

Representa a configuração de taxa de transferência máxima (pico) do grupo de políticas de qualidade do serviço (QoS) de storage atribuído ao workload. Se o componente do grupo de políticas estiver na contenção, isso significa que todas as cargas de trabalho no grupo de políticas estão sendo controladas pelo limite de taxa de transferência definido, o que está impactando a latência de uma ou mais dessas cargas de trabalho.

- **Limite de QoS min**

Representa a latência de um workload que está sendo causado pela configuração mínima (esperada) de taxa de transferência de QoS atribuída a outros workloads. Se o conjunto mínimo de QoS em certos workloads usar a maior parte da largura de banda para garantir a taxa de transferência prometida, outros workloads serão controlados e verão mais latência.

- **Interconexão de cluster**

Representa os cabos e adaptadores com os quais os nós em cluster estão fisicamente conectados. Se o componente de interconexão de cluster estiver na contenção, isso significa que o tempo de espera alto para solicitações de e/S na interconexão de cluster está impactando a latência de um ou mais workloads.

- **Data Processing**

Representa o componente de software no cluster envolvido com o processamento de e/S entre o cluster e o agregado de storage que contém a carga de trabalho. O Data Processing de tratamento do nó pode ter sido alterado desde que o evento foi detectado. Se o componente Data Processing estiver em contenção,

isso significa que a alta utilização no nó Data Processing está impactando a latência de um ou mais workloads.

- **\* Ativação de volume\***

Representa o processo que controla o uso de todos os volumes ativos. Em ambientes grandes onde mais de 1000 volumes estão ativos, esse processo controla quantos volumes críticos precisam acessar recursos por meio do nó ao mesmo tempo. Quando o número de volumes ativos simultâneos exceder o limite máximo recomendado, alguns dos volumes não críticos terão latência conforme identificado aqui.

- **Recursos MetroCluster**

Representa os recursos do MetroCluster, incluindo NVRAM e links interswitches (ISLs), usados para espelhar dados entre clusters em uma configuração do MetroCluster. Se o componente MetroCluster estiver em contenção, isso significa que a alta taxa de transferência de gravação de workloads no cluster local ou um problema de integridade de link está impactando a latência de um ou mais workloads no cluster local. Se o cluster não estiver em uma configuração do MetroCluster, este ícone não será exibido.

- **Operações agregadas ou SSD agregadas**

Representa o agregado de storage no qual os workloads estão sendo executados. Se o componente agregado estiver na contenção, isso significa que a alta utilização no agregado está impactando a latência de um ou mais workloads. Um agregado consiste em todos os HDDs, ou uma combinação de HDDs e SSDs (agregado de Flash Pool), ou uma combinação de HDDs e uma camada de nuvem (agregado de FabricPool). Um "agregado SSD" consiste em todos os SSDs (um agregado all-flash) ou uma combinação de SSDs e uma camada de nuvem (agregado FabricPool).

- **Latência da nuvem**

Representa o componente de software no cluster envolvido com o processamento de e/S entre o cluster e a camada de nuvem na qual os dados do usuário são armazenados. Se o componente de latência da nuvem estiver em contenção, isso significa que uma grande quantidade de leituras de volumes hospedados na camada de nuvem está impactando a latência de um ou mais workloads.

- **Sincronizar SnapMirror**

Representa o componente de software no cluster envolvido com a replicação dos dados do usuário do volume primário para o volume secundário em uma relação síncrona do SnapMirror. Se o componente Sync SnapMirror estiver na contenção, isso significa que a atividade das operações síncronas do SnapMirror está impactando a latência de um ou mais workloads.

## **Funções dos workloads envolvidos em um evento de desempenho**

O Unified Manager usa funções para identificar o envolvimento de um workload em um evento de performance. Os papéis incluem vítimas, agressores e tubarões. Uma carga de trabalho definida pelo usuário pode ser uma vítima, um valentão e um tubarão ao mesmo tempo.

Função	Descrição
Vítima	Uma carga de trabalho definida pelo usuário cujo desempenho diminuiu devido a outras cargas de trabalho, chamadas de bullies, que usam excessivamente um componente de cluster. Somente cargas de trabalho definidas pelo usuário são identificadas como vítimas. O Unified Manager identifica os workloads da vítima com base em seu desvio na latência, em que a latência real, durante um evento, aumentou muito em relação à previsão de latência (intervalo esperado).
Bully	Uma carga de trabalho definida pelo usuário ou definida pelo sistema cujo uso excessivo de um componente de cluster causou a diminuição do desempenho de outras cargas de trabalho, chamadas vítimas. O Unified Manager identifica cargas de trabalho bully com base em seu desvio no uso de um componente do cluster, em que o uso real, durante um evento, aumentou muito em relação ao intervalo de uso esperado.
Tubarão	Um workload definido pelo usuário com a maior utilização de um componente de cluster em comparação a todas as cargas de trabalho envolvidas em um evento. O Unified Manager identifica workloads de tubarão com base no uso de um componente de cluster durante um evento.

Os workloads em um cluster podem compartilhar muitos dos componentes do cluster, como agregados e CPU para rede e Data Processing. Quando uma carga de trabalho, como um volume, aumenta o uso de um componente de cluster a ponto de que o componente não pode atender com eficiência às demandas de workload, o componente está em contenção. A carga de trabalho que está usando um componente de cluster é um bully. As outras cargas de trabalho que compartilham esses componentes, e cujo desempenho é afetado pelo agressor, são as vítimas. As atividades de workloads definidos pelo sistema, como deduplicação ou cópias Snapshot, também podem escalar para "bullying".

Quando o Unified Manager detecta um evento, ele identifica todos os workloads e componentes de cluster envolvidos, incluindo os workloads bully que causaram o evento, o componente do cluster que está em contenção e os workloads da vítima cujo desempenho diminuiu devido ao aumento da atividade dos workloads bully.



Se o Unified Manager não conseguir identificar os workloads bully, ele só alertará sobre os workloads da vítima e o componente do cluster envolvido.

O Unified Manager pode identificar workloads vítimas de workloads bully e também identificar quando esses mesmos workloads se tornam workloads bully. Uma carga de trabalho pode ser um bully para si mesma. Por exemplo, uma carga de trabalho de alta performance que está sendo controlada por um limite de grupo de políticas faz com que todas as cargas de trabalho no grupo de políticas sejam limitadas, incluindo a própria. Uma carga de trabalho que é um agressor ou uma vítima em um evento de desempenho contínuo pode mudar sua função ou não ser mais um participante no evento.

# Gerenciamento dos limites de performance

As políticas de limite de performance permitem determinar o ponto em que o Unified Manager gera um evento para informar os administradores de sistema sobre problemas que podem estar afetando a performance do workload. Essas políticas de limite são conhecidas como limites de desempenho *definidos pelo usuário*.

Esta versão é compatível com limites de desempenho dinâmico, definido pelo sistema e definido pelo usuário. Com limites de performance dinâmicos e definidos pelo sistema, o Unified Manager analisa a atividade do workload para determinar o valor de limite apropriado. Com limites definidos pelo usuário, você pode definir os limites de desempenho superiores para muitos contadores de performance e para muitos objetos de storage.



Os limites de performance definidos pelo sistema e os limites de performance dinâmica são definidos pelo Unified Manager e não são configuráveis. Se você estiver recebendo eventos desnecessários de qualquer política de limite de desempenho definido pelo sistema, poderá desativar políticas individuais na página Configuração de eventos.

## Como funcionam as políticas de limite de performance definidas pelo usuário

Você define políticas de limite de performance em objetos de storage (por exemplo, em agregados e volumes) para que um evento possa ser enviado ao administrador de storage para informar ao administrador de que o cluster está com um problema de performance.

Você cria uma política de limite de performance para um objeto de storage ao:

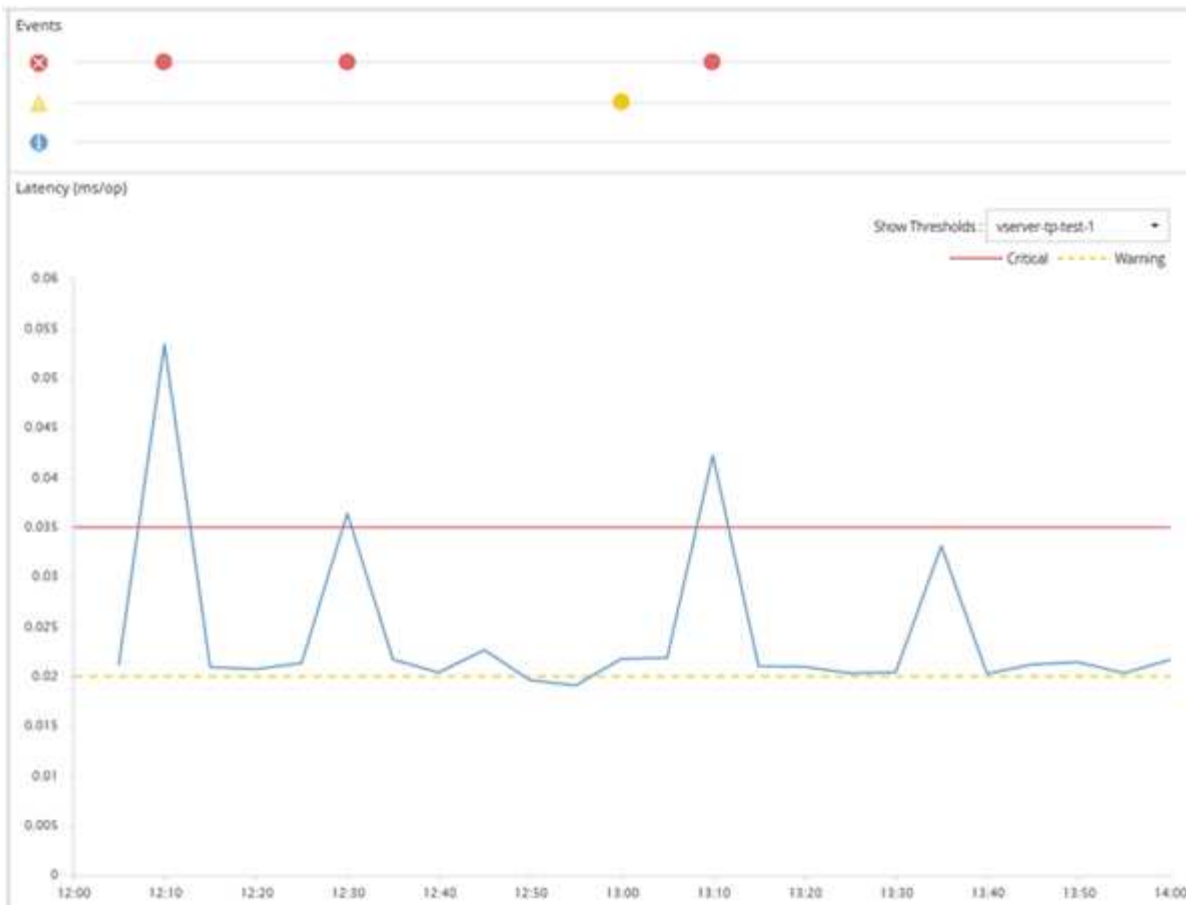
- Selecionar um objeto de armazenamento
- Selecionar um contador de desempenho associado a esse objeto
- Especificar valores que definem os limites superiores do contador de desempenho considerados situações críticas e de aviso
- Especificar um período de tempo que define quanto tempo o contador deve exceder o limite superior

Por exemplo, você pode definir uma política de limite de desempenho em um volume para receber uma notificação de evento crítico sempre que o IOPS desse volume exceder 750 operações por segundo por 10 minutos consecutivos. Essa mesma política de limite também pode especificar que um evento de aviso seja enviado quando o IOPS exceder 500 operações por segundo por 10 minutos.



A versão atual fornece limites que enviam eventos quando um valor de contador excede a configuração de limite. Você não pode definir limites que enviam eventos quando um valor de contador cai abaixo de uma configuração de limite.

Um exemplo de gráfico de contador é mostrado aqui, indicando que um limite de aviso (ícone amarelo) foi violado às 1:00, e que um limite crítico (ícone vermelho) foi violado às 12:10, 12:30 e 1:10:



Uma violação de limite deve ocorrer continuamente durante a duração especificada. Se o limiar cair abaixo dos valores-limite por qualquer motivo, uma violação subsequente é considerada o início de uma nova duração.

Alguns objetos de cluster e contadores de performance permitem criar uma política de limite de combinação que exige que dois contadores de desempenho excedam seus limites máximos antes que um evento seja gerado. Por exemplo, você pode criar uma política de limite usando os seguintes critérios:

Objeto de cluster	Contador de desempenho	Limite de aviso	Limite crítico	Duração
Volume	Latência	10 milissegundos	20 milissegundos	15 minutos
Agregado	Utilização	65%	85%	

As políticas de limite que usam dois objetos de cluster fazem com que um evento seja gerado somente quando ambas as condições forem violadas. Por exemplo, usando a política de limite definida na tabela:

Se a latência do volume estiver na média...	E a utilização agregada do disco é...	Então...
15 milissegundos	50%	Nenhum evento é comunicado.
15 milissegundos	75%	É comunicado um evento de aviso.

Se a latência do volume estiver na média...	E a utilização agregada do disco é...	Então...
25 milissegundos	75%	É comunicado um evento de aviso.
25 milissegundos	90%	É comunicado um evento crítico.

## O que acontece quando uma política de limite de desempenho é violada

Quando um valor de contador excede seu valor limite de desempenho definido pelo período de tempo especificado na duração, o limite é violado e um evento é relatado.

O evento faz com que as seguintes ações sejam iniciadas:

- O evento é exibido no Painel de Controle, na página Resumo do cluster de desempenho, na página Eventos e na página Inventário de desempenho específico do objeto.
- (Opcional) um alerta de e-mail sobre o evento pode ser enviado para um ou mais destinatários de e-mail e uma armadilha SNMP pode ser enviada para um recetor de armadilha.
- (Opcional) Um script pode ser executado para modificar ou atualizar automaticamente objetos de armazenamento.

A primeira ação é sempre executada. Você configura se as ações opcionais são executadas na página Configuração de alerta. Você pode definir ações exclusivas dependendo se uma política de aviso ou limite crítico for violada.

Após uma violação de política de limite de desempenho ter ocorrido em um objeto de armazenamento, não serão gerados mais eventos para essa política até que o valor do contador fique abaixo do valor limite, momento em que a duração é redefinida para esse limite. Embora o limite continue a ser excedido, a hora de término do evento é continuamente atualizada para refletir que esse evento está em andamento.

Um evento de limite captura ou congela as informações relacionadas à gravidade e à definição de política para que as informações de limite exclusivas sejam exibidas com o evento, mesmo que a política de limite seja modificada no futuro.

## Quais contadores de desempenho podem ser rastreados usando limites

Alguns contadores de desempenho comuns, como IOPS e MB/s, podem ter limites definidos para todos os objetos de armazenamento. Existem outros contadores que podem ter limites definidos apenas para determinados objetos de armazenamento.

### Contadores de desempenho disponíveis

Objeto de storage	Contador de desempenho	Descrição
Cluster	IOPS	Número médio de operações de entrada/saída que o cluster processa por segundo.

<b>Objeto de storage</b>	<b>Contador de desempenho</b>	<b>Descrição</b>
MB/s	Número médio de megabytes de dados transferidos de e para este cluster por segundo.	Nó
IOPS	Número médio de operações de entrada/saída que o nó processa por segundo.	MB/s
Número médio de megabytes de dados transferidos de e para este nó por segundo.	Latência	Número médio de milissegundos que o nó leva para responder às solicitações de aplicação.
Utilização	Porcentagem média da CPU e RAM do nó que está sendo usado.	Capacidade de performance utilizada
Porcentagem média de capacidade de performance consumida pelo nó.	Capacidade de desempenho utilizada - takeover	Porcentagem média de capacidade de performance consumida pelo nó e a capacidade de performance do nó do parceiro.
Agregado	IOPS	Número médio de operações de entrada/saída os processos agregados por segundo.
MB/s	Número médio de megabytes de dados transferidos de e para este agregado por segundo.	Latência
Número médio de milissegundos que o agregado leva para responder às solicitações do aplicativo.	Utilização	Porcentagem média dos discos do agregado que estão sendo usados.
Capacidade de performance utilizada	Porcentagem média de capacidade de performance consumida pelo agregado.	Armazenamento VM
IOPS	Número médio de operações de entrada/saída processadas pelo SVM por segundo.	MB/s
Número médio de megabytes de dados transferidos de e para este SVM por segundo.	Latência	Número médio de milissegundos que o SVM leva para responder a solicitações de aplicações.



<b>Objeto de storage</b>	<b>Contador de desempenho</b>	<b>Descrição</b>
Volume	IOPS	Número médio de operações de entrada/saída o volume processa por segundo.
MB/s	Número médio de megabytes de dados transferidos de e para este volume por segundo.	Latência
Número médio de milissegundos que o volume leva para responder às solicitações do aplicativo.	Relação de falta de cache	Porcentagem média de solicitações de leitura de aplicativos clientes que são retornadas do volume em vez de serem retornadas do cache.
LUN	IOPS	Número médio de operações de entrada/saída que o LUN processa por segundo.
MB/s	Número médio de megabytes de dados transferidos de e para este LUN por segundo.	Latência
Número médio de milissegundos que o LUN leva para responder às solicitações de aplicativos.	Namespace	IOPS
Número médio de operações de entrada/saída que o namespace processa por segundo.	MB/s	Número médio de megabytes de dados transferidos para e a partir deste namespace por segundo.
Latência	Número médio de milissegundos que o namespace leva para responder a solicitações de aplicativos.	Porta
Utilização de largura de banda	Porcentagem média da largura de banda disponível da porta que está sendo usada.	MB/s
Número médio de megabytes de dados transferidos para e a partir desta porta por segundo.	Interface de rede (LIF)	MB/s

## **Quais objetos e contadores podem ser usados em políticas de limite de combinação**

Apenas alguns contadores de desempenho podem ser usados em conjunto em políticas de combinação. Quando os contadores de desempenho primário e secundário são

especificados, ambos os contadores de desempenho devem exceder seus limites máximos antes que um evento seja gerado.

Objeto de armazenamento primário e contador	Objeto e contador de armazenamento secundário
Latência de volume	IOPS do volume
Volume MB/s	Utilização de agregado
Capacidade de desempenho agregado usada	Utilização do nó
Capacidade de performance do nó usada	Capacidade de desempenho do nó usada - takeover
Latência de LUN	IOPS LUN
MB/s LUN	Utilização de agregado
Capacidade de desempenho agregado usada	Utilização do nó
Capacidade de performance do nó usada	Capacidade de desempenho do nó usada - takeover



Quando uma política de combinação de volume é aplicada a um volume FlexGroup, em vez de a um FlexVol volume, apenas os atributos "IOPS de volume" e "volume MB/s" podem ser selecionados como o contador secundário. Se a política de limite contiver um dos atributos de nó ou agregado, a política não será aplicada ao volume FlexGroup e você receberá uma mensagem de erro descrevendo esse caso. Isso ocorre porque os volumes do FlexGroup podem existir em mais de um nó ou agregado.

## Criação de políticas de limite de performance definidas pelo usuário

Você cria políticas de limite de desempenho para objetos de armazenamento de modo que as notificações sejam enviadas quando um contador de desempenho exceder um valor específico. A notificação de evento identifica que o cluster está enfrentando um problema de desempenho.

### Antes de começar

Tem de ter a função Administrador de aplicações.

Você cria políticas de limite de desempenho inserindo os valores de limite na página criar política de limite de desempenho. Você pode criar novas políticas definindo todos os valores de política nesta página ou pode fazer uma cópia de uma política existente e alterar os valores na cópia (chamada *clonagem*).

Os valores-limite válidos são de 0,001 a 10.000.000 para números, 0.001-100 para porcentagens e 0.001-200 para porcentagens de capacidade de desempenho usada.



A versão atual fornece limites que enviam eventos quando um valor de contador excede a configuração de limite. Você não pode definir limites que enviam eventos quando um valor de contador cai abaixo de uma configuração de limite.

## Passos

1. No painel de navegação esquerdo, selecione **limites de eventos > desempenho**.

É apresentada a página limites de desempenho.

2. Clique no botão apropriado dependendo se você deseja criar uma nova política ou se deseja clonar uma política semelhante e modificar a versão clonada.

Para...	Clique em...
Crie uma nova política	<b>Criar</b>
Clonar uma política existente	Selecione uma política existente e clique em <b>Clone</b>

A página criar política de limite de desempenho ou a página clonar política de limite de desempenho é exibida.

3. Defina a política de limite especificando os valores de limite do contador de desempenho que deseja definir para objetos de armazenamento específicos:
  - a. Selecione o tipo de objeto de armazenamento e especifique um nome e uma descrição para a política.
  - b. Selecione o contador de desempenho a ser rastreado e especifique os valores limite que definem eventos de Aviso e Crítica.

Tem de definir pelo menos um aviso ou um limite crítico. Não é necessário definir ambos os tipos de limites.

- c. Selecione um contador de desempenho secundário, se necessário, e especifique os valores limite para eventos de Aviso e Crítica.

A inclusão de um contador secundário exige que ambos os contadores excedam os valores limite antes que o limite seja violado e um evento seja relatado. Somente determinados objetos e contadores podem ser configurados usando uma política de combinação.

- d. Selecione a duração do tempo para o qual os valores-limite devem ser violados para que um evento seja enviado.

Ao clonar uma política existente, você deve inserir um novo nome para a política.

4. Clique em **Salvar** para salvar a política.

Você retorna à página limites de desempenho. Uma mensagem de sucesso na parte superior da página confirma que a diretiva de limite foi criada e fornece um link para a página Inventário para esse tipo de objeto para que você possa aplicar a nova diretiva a objetos de armazenamento imediatamente.

Se você quiser aplicar a nova diretiva de limite a objetos de armazenamento neste momento, clique no link **ir para object\_type now** para ir para a página Inventário.

## Atribuindo políticas de limite de desempenho a objetos de storage

Você atribui uma política de limite de desempenho definido pelo usuário a um objeto de storage para que o Unified Manager relate um evento se o valor do contador de

desempenho exceder a configuração de política.

### Antes de começar

Tem de ter a função Administrador de aplicações.

A política de limite de desempenho, ou políticas, que você deseja aplicar ao objeto, deve existir.

Você pode aplicar apenas uma política de desempenho de cada vez a um objeto ou a um grupo de objetos.

É possível atribuir um máximo de três políticas de limite a cada objeto de storage. Ao atribuir políticas a vários objetos, se algum dos objetos já tiver o número máximo de políticas atribuído, o Unified Manager executará as seguintes ações:

- Aplica a política a todos os objetos selecionados que não atingiram o seu máximo
- Ignora os objetos que atingiram o número máximo de políticas
- Exibe uma mensagem informando que a diretiva não foi atribuída a todos os objetos

### Passos

1. Na página inventário de desempenho de qualquer objeto de storage, selecione o objeto ou objetos aos quais você deseja atribuir uma política de limite:

Para atribuir limites a...	Clique em...
Um único objeto	A caixa de verificação à esquerda desse objeto.
Vários objetos	A caixa de verificação à esquerda de cada objeto.
Todos os objetos na página	A <input type="checkbox"/> caixa suspensa e escolha <b>Selecione todos os objetos nesta página.</b>
Todos os objetos do mesmo tipo	A <input type="checkbox"/> caixa suspensa e escolha <b>Selecionar todos os objetos.</b>

Você pode usar a funcionalidade de classificação e filtragem para refinar a lista de objetos na página de inventário para facilitar a aplicação de políticas de limite a muitos objetos.

2. Faça sua seleção e clique em **Assign Performance Threshold Policy**.

A página atribuir política de limite de desempenho é exibida, mostrando uma lista de políticas de limite que existem para esse tipo específico de objeto de storage.

3. Clique em cada política para exibir os detalhes das configurações de limite de desempenho para verificar se você selecionou a política de limite correta.
4. Depois de selecionar a política de limite apropriada, clique em **Assign Policy** (atribuir política).

Uma mensagem de sucesso na parte superior da página confirma que a diretiva de limite foi atribuída ao objeto ou objetos e fornece um link para a página de alertas para que você possa configurar as configurações de alerta para esse objeto e política.

Se você quiser que os alertas sejam enviados por e-mail ou como uma armadilha SNMP, para notificá-lo de que um evento de desempenho específico foi gerado, você deve configurar as configurações de alerta na

página Configuração de alerta.

## Exibindo políticas de limite de desempenho

Você pode exibir todas as políticas de limite de desempenho definidas atualmente na página limites de desempenho.

A lista de políticas de limite é ordenada alfabeticamente por nome de política e inclui políticas para todos os tipos de objetos de storage. Você pode clicar em um cabeçalho de coluna para classificar as políticas por essa coluna. Se você estiver procurando uma política específica, use os mecanismos de filtro e pesquisa para refinar a lista de políticas de limite que aparecem na lista de inventário.

Você pode passar o cursor sobre o Nome da política e o nome da condição para ver os detalhes de configuração da política. Além disso, você pode usar os botões fornecidos para criar, clonar, editar e excluir políticas de limite definidas pelo usuário.

### Passo

1. No painel de navegação esquerdo, selecione **limiares de eventos > desempenho**.

É apresentada a página limites de desempenho.

## Editando políticas de limite de performance definidas pelo usuário

Você pode editar as configurações de limite para as políticas de limite de desempenho existentes. Isso pode ser útil se você achar que está recebendo muitos ou poucos alertas para determinadas condições de limite.

### Antes de começar

Tem de ter a função Administrador de aplicações.

Não é possível alterar o nome da política ou o tipo de objeto de armazenamento que está sendo monitorado para políticas de limite existentes.

### Passos

1. No painel de navegação esquerdo, selecione **limiares de eventos > desempenho**.

A página limites de desempenho é exibida.

2. Selecione a política de limite que deseja alterar e clique em **Editar**.

A página Editar política de limite de desempenho é exibida.

3. Faça suas alterações na política de limite e clique em **Salvar**.

Você retorna à página limites de desempenho.

Depois que eles são salvos, as alterações são atualizadas imediatamente em todos os objetos de armazenamento que usam a diretiva.

Dependendo do tipo de alterações feitas na política, talvez você queira revisar as configurações de alerta configuradas para os objetos que usam a política na página Configuração de alerta.

## Remoção de políticas de limite de performance de objetos de storage

Você pode remover uma política de limite de performance definida pelo usuário de um objeto de storage quando não quiser mais que o Unified Manager monitore o valor do contador de performance.

### Antes de começar

Tem de ter a função Administrador de aplicações.

Você pode remover apenas uma política de cada vez de um objeto selecionado.

Você pode remover uma política de limite de vários objetos de armazenamento selecionando mais de um objeto na lista.

### Passos

1. Na página **inventário** de qualquer objeto de armazenamento, selecione um ou mais objetos que tenham pelo menos uma política de limite de desempenho aplicada.

Para limpar limites de...	Faça isso...
Um único objeto	Marque a caixa de seleção à esquerda desse objeto.
Vários objetos	Marque a caixa de seleção à esquerda de cada objeto.
Todos os objetos na página	Clique <input type="checkbox"/> no cabeçalho da coluna.

2. Clique em **Limpar política de limite de desempenho**.

A página Limpar política de limite é exibida, mostrando uma lista de políticas de limite que estão atualmente atribuídas aos objetos de armazenamento.

3. Selecione a política de limite que deseja remover dos objetos e clique em **Limpar Política**.

Quando você seleciona uma política de limite, os detalhes da política são exibidos para que você possa confirmar que selecionou a política apropriada.

## O que acontece quando uma política de limite de desempenho é alterada

Se você ajustar o valor do contador ou a duração de uma política de limite de desempenho existente, a alteração de política será aplicada a todos os objetos de armazenamento que usam a diretiva. A nova configuração ocorre imediatamente e o Unified Manager começa a comparar os valores do contador de desempenho com as novas configurações de limite para todos os dados de desempenho recém-coletados.

Se existirem eventos ativos para objetos que estejam usando a política de limite alterada, os eventos serão marcados como obsoletos e a política de limite começará a monitorar o contador como uma política de limite recém-definida.

Ao visualizar o contador no qual o limite foi aplicado na Exibição detalhada dos gráficos de Contador, as linhas de limite crítico e de aviso refletem as configurações de limite atuais. As configurações de limite originais não aparecem nesta página, mesmo que você exiba dados históricos quando a configuração de limite antiga estava em vigor.



Como as configurações de limite mais antigas não aparecem na Exibição detalhada dos gráficos de Contador, você pode ver eventos históricos que aparecem abaixo das linhas de limite atuais.

## O que acontece com as políticas de limite de performance quando um objeto é movido

Como as políticas de limite de performance são atribuídas a objetos de storage, se você mover um objeto, todas as políticas de limite atribuídas permanecerão anexadas ao objeto após a conclusão da migração. Por exemplo, se você mover um volume ou LUN para um agregado diferente, as políticas de limite ainda estarão ativas para o volume ou LUN no novo agregado.

Se existir uma condição de contador secundário para a política de limite (uma política de combinação)—por exemplo, se uma condição adicional for atribuída a um agregado ou a um nó—a condição de contador secundário é aplicada ao novo agregado ou nó para o qual o volume ou LUN foi movido.

Se houver novos eventos ativos para objetos que estejam usando a política de limite alterada, os eventos serão marcados como obsoletos e a política de limite começará a monitorar o contador como uma política de limite recém-definida.

Uma operação de movimentação de volume faz com que o ONTAP envie um evento de mudança informativa. Um ícone de evento de mudança é exibido na linha do tempo de eventos na página Performance Explorer e na página análise de carga de trabalho para indicar a hora em que a operação de movimentação foi concluída.



Se você mover um objeto para um cluster diferente, a política de limite definida pelo usuário será removida do objeto. Se necessário, você deve atribuir uma política de limite ao objeto depois que a operação mover for concluída. No entanto, as políticas de limite dinâmicas e definidas pelo sistema são aplicadas automaticamente a um objeto depois que ele é movido para um novo cluster.

## Funcionalidade de política de limite durante o takeover de HA e a giveback

Quando uma operação de takeover ou giveback ocorre em uma configuração de alta disponibilidade (HA), os objetos movidos de um nó para o outro nó mantêm suas políticas de limite da mesma maneira que nas operações de movimentação manual. Como o Unified Manager verifica se há alterações na configuração do cluster a cada 15 minutos, o impacto do switchover para o novo nó não é identificado até a próxima votação da configuração de cluster.



Se uma operação de aquisição e giveback ocorrerem dentro do período de coleta de alterações de configuração de 15 minutos, talvez as estatísticas de desempenho não sejam exibidas de um nó para o outro.

## Funcionalidade de política de limite durante a realocação de agregados

Se você mover um agregado de um nó para outro usando o `aggregate relocation start` comando, as políticas de limite único e de combinação serão mantidas em todos os objetos e a parte do nó da política de limite será aplicada ao novo nó.

## Funcionalidade de política de limite durante o switchover do MetroCluster

Os objetos que se movem de um cluster para outro cluster em uma configuração do MetroCluster não mantêm suas configurações de política de limite definidas pelo usuário. Se necessário, você pode aplicar políticas de limite nos volumes e LUNs movidos para o cluster de parceiros. Depois que um objeto é movido de volta para o cluster original, a política de limite definida pelo usuário é reaplicada automaticamente.

Para obter informações, "[Comportamento do volume durante o switchover e o switchback](#)" consulte .

## Analizando eventos de desempenho

Você pode analisar eventos de desempenho para identificar quando eles foram detetados, se eles estão ativos (novos ou reconhecidos) ou obsoletos, as cargas de trabalho e os componentes de cluster envolvidos e as opções para resolver os eventos por conta própria.

## Exibindo informações sobre eventos de desempenho

Você pode usar a página de inventário de gerenciamento de eventos para exibir uma lista de todos os eventos de desempenho nos clusters que estão sendo monitorados pelo Unified Manager. Ao visualizar essas informações, você pode determinar os eventos mais críticos e, em seguida, detalhar informações detalhadas para determinar a causa do evento.

### Antes de começar

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

A lista de eventos é ordenada por hora detetada, com os eventos mais recentes listados primeiro. Você pode clicar em um cabeçalho de coluna para classificar os eventos com base nessa coluna. Por exemplo, você pode classificar pela coluna Status para exibir eventos por gravidade. Se você está procurando um evento específico ou um tipo específico de evento, você pode usar os mecanismos de filtro e pesquisa para refinar a lista de eventos que aparecem na lista.

Eventos de todas as fontes são exibidos nesta página:

- Política de limite de desempenho definido pelo usuário
- Política de limite de desempenho definido pelo sistema
- Limite de desempenho dinâmico

A coluna tipo de evento lista a origem do evento. Você pode selecionar um evento para exibir detalhes sobre o evento na página de detalhes do evento.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.



2. No menu Exibir, selecione **Eventos de desempenho ativo**.

A página exibe todos os eventos de desempenho novo e reconhecido que foram gerados nos últimos 7 dias.

3. Localize um evento que você deseja analisar e clique no nome do evento.

A página de detalhes do evento é exibida.



Você também pode exibir a página de detalhes de um evento clicando no link do nome do evento na página do Performance Explorer e em um e-mail de alerta.

## Analizando eventos a partir de limites de desempenho definidos pelo usuário

Os eventos gerados a partir de limites definidos pelo usuário indicam que um contador de desempenho para um determinado objeto de storage, por exemplo, um agregado ou volume, ultrapassou o limite definido na política. Isso indica que o objeto de cluster está enfrentando um problema de desempenho.

Você usa a página de detalhes do evento para analisar o evento de desempenho e tomar medidas corretivas, se necessário, para retornar o desempenho ao normal.

### Resposta a eventos de limite de desempenho definidos pelo usuário

Você pode usar o Unified Manager para investigar eventos de desempenho causados por um contador de desempenho que atravessa um aviso definido pelo usuário ou um limite crítico. Você também pode usar o Unified Manager para verificar a integridade do componente do cluster para ver se eventos recentes de integridade detetados no componente contribuíram para o evento de desempenho.

#### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Deve haver eventos de desempenho novos ou obsoletos.

#### Passos

1. Exiba a página **Detalhes do evento** para exibir informações sobre o evento.
2. Revise a **Descrição**, que descreve a violação de limite que causou o evento.

Por exemplo, a mensagem "valor de latência de 456 ms/op acionou um evento DE AVISO baseado na configuração de limite de 400 ms/op" indica que ocorreu um evento de aviso de latência para o objeto.

3. Passe o cursor sobre o nome da política para exibir detalhes sobre a política de limite que acionou o evento.

Isso inclui o nome da política, o contador de desempenho sendo avaliado, o valor do contador que deve ser violado para ser considerado um evento crítico ou de aviso e a duração pela qual o contador deve exceder o valor.

4. Anote o **Event Trigger Time** para que você possa investigar se outros eventos podem ter ocorrido ao mesmo tempo que poderiam ter contribuído para este evento.

5. Siga uma das opções abaixo para investigar mais o evento, para determinar se você precisa executar alguma ação para resolver o problema de desempenho:

Opção	Possíveis ações de investigação
Clique no nome do objeto fonte para exibir a página Explorer para esse objeto.	Esta página permite exibir os detalhes do objeto e comparar esse objeto com outros objetos de armazenamento semelhantes para ver se outros objetos de armazenamento têm um problema de desempenho ao mesmo tempo. Por exemplo, para ver se outros volumes no mesmo agregado também estão tendo um problema de desempenho.
Clique no nome do cluster para exibir a página Resumo do cluster.	Esta página permite exibir os detalhes do cluster no qual esse objeto reside para ver se outros problemas de desempenho ocorreram ao mesmo tempo.

## Analizando eventos a partir de limites de desempenho definidos pelo sistema

Os eventos gerados a partir dos limites de desempenho definidos pelo sistema indicam que um contador de desempenho ou um conjunto de contadores de desempenho para um determinado objeto de storage ultrapassou o limite de uma política definida pelo sistema. Isso indica que o objeto de storage, por exemplo, um agregado ou nó, está enfrentando um problema de desempenho.

Você usa a página de detalhes do evento para analisar o evento de desempenho e tomar medidas corretivas, se necessário, para retornar o desempenho ao normal.



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

## Resposta a eventos de limite de desempenho definido pelo sistema

Você pode usar o Unified Manager para investigar eventos de desempenho causados por um contador de desempenho que cruza um limite de aviso definido pelo sistema. Você também pode usar o Unified Manager para verificar a integridade do componente do cluster para ver se os eventos recentes detectados no componente contribuíram para o evento de desempenho.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Deve haver eventos de desempenho novos ou obsoletos.

### Passos

1. Exiba a página **Detalhes do evento** para exibir informações sobre o evento.
2. Revise a **Descrição**, que descreve a violação de limite que causou o evento.

Por exemplo, a mensagem "'valor de utilização do nó de 90 % desencadeou um evento DE AVISO baseado na definição de limite de 85 %'" indica que ocorreu um evento de aviso de utilização do nó para o objeto de cluster.

3. Anote o **Event Trigger Time** para que você possa investigar se outros eventos podem ter ocorrido ao mesmo tempo que poderiam ter contribuído para este evento.
4. Em **Diagnóstico do sistema**, reveja a breve descrição do tipo de análise que a política definida pelo sistema está a executar no objeto de cluster.

Para alguns eventos, é apresentado um ícone verde ou vermelho junto do diagnóstico para indicar se foi encontrado um problema nesse diagnóstico específico. Para outros tipos de gráficos de contador de eventos definidos pelo sistema, é apresentado o desempenho do objeto.

5. Em **ações sugeridas**, clique no link **Ajude-me a fazer isso** para exibir as ações sugeridas que você pode executar para tentar resolver o evento de desempenho por conta própria.

### Resposta a eventos de desempenho do grupo de políticas de QoS

O Unified Manager gera eventos de aviso de política de QoS quando a taxa de transferência de workload (IOPS, IOPS/TB ou Mbps) excedeu a configuração definida de política de QoS ONTAP e a latência de workload está sendo afetada. Esses eventos definidos pelo sistema oferecem a oportunidade de corrigir possíveis problemas de desempenho antes que muitos workloads sejam afetados pela latência.

#### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Deve haver eventos de desempenho novos, reconhecidos ou obsoletos.

O Unified Manager gera eventos de aviso para violações de política de QoS quando a taxa de transferência de workload excede a configuração de política de QoS definida durante cada período de coleta de performance da hora anterior. A taxa de transferência do workload pode exceder o limite de QoS por apenas um curto período de tempo durante cada período de coleta, mas o Unified Manager exibe somente a taxa de transferência "'média'" durante o período de coleta no gráfico. Por esse motivo, você pode receber eventos de QoS enquanto a taxa de transferência de uma carga de trabalho pode não ter cruzado o limite de política mostrado no gráfico.

Você pode usar o Gerenciador do sistema ou os comandos ONTAP para gerenciar grupos de políticas, incluindo as seguintes tarefas:

- Criando um novo grupo de políticas para a carga de trabalho
- Adição ou remoção de cargas de trabalho em um grupo de políticas
- Movimentação de uma carga de trabalho entre grupos de políticas
- Alterar o limite de taxa de transferência de um grupo de políticas
- Movendo um workload para um agregado ou nó diferente

#### Passos

1. Exiba a página **Detalhes do evento** para exibir informações sobre o evento.
2. Revise a **Descrição**, que descreve a violação de limite que causou o evento.

Por exemplo, a mensagem "'valor de IOPS de 1.352 IOPS no vol1\_NFS1 disparou um evento DE AVISO

para identificar possíveis problemas de desempenho para o workload"" indica que um evento de IOPS máximo de QoS ocorreu no volume vol1\_NFS1.

3. Consulte a seção **informações do evento** para ver mais detalhes sobre quando o evento ocorreu e por quanto tempo o evento esteve ativo.

Além disso, para volumes ou LUNs que compartilham a taxa de transferência de uma política de QoS, você pode ver os nomes dos três principais workloads que consomem a maior parte do IOPS ou Mbps.

4. Na seção **Diagnóstico do sistema**, revise os dois gráficos: Um para IOPS médio total ou Mbps (dependendo do evento) e outro para latência. Quando organizado dessa maneira, você pode ver quais componentes do cluster estão mais afetando a latência quando o workload chegou ao limite máximo de QoS.

Para um evento de política de QoS compartilhada, os três principais workloads são mostrados no gráfico de taxa de transferência. Se mais de três workloads estiverem compartilhando a política de QoS, workloads adicionais serão adicionados em uma categoria "outras cargas de trabalho". Além disso, o gráfico de latência mostra a latência média em todos os workloads que fazem parte da política de QoS.

Observe que, para eventos de política de QoS adaptável, os gráficos IOPS e Mbps mostram valores de IOPS ou Mbps convertidos pelo ONTAP da diretiva de limite de IOPS/TB atribuída com base no tamanho do volume.

5. Na seção **ações sugeridas**, revise as sugestões e determine quais ações você deve executar para evitar um aumento na latência da carga de trabalho.

Se necessário, clique no botão **Ajuda** para ver mais detalhes sobre as ações sugeridas que você pode executar para tentar resolver o evento de desempenho.

## Entendendo eventos de políticas de QoS adaptáveis que têm um tamanho de bloco definido

Os grupos de políticas de QoS adaptáveis escalam automaticamente um limite de taxa de transferência ou um piso com base no tamanho do volume, mantendo a proporção de IOPS para TBs conforme o tamanho do volume muda. A partir do ONTAP 9.5, você pode especificar o tamanho do bloco na política de QoS para aplicar efetivamente um limite de MB/s ao mesmo tempo.

A atribuição de um limite de IOPS em uma política de QoS adaptável coloca um limite apenas no número de operações que ocorrem em cada workload. Dependendo do tamanho do bloco definido no cliente que gera as cargas de trabalho, alguns IOPS incluem muito mais dados e, portanto, colocam uma carga muito maior sobre os nós que processam as operações.

O valor MB/s para uma carga de trabalho é gerado usando a seguinte fórmula:

$$\text{MB/s} = (\text{IOPS} * \text{Block Size}) / 1000$$

Se uma carga de trabalho estiver com uma média de 3.000 IOPS e o tamanho do bloco no cliente estiver definido para 32 KB, os MB/s efetivos para essa carga de trabalho serão 96. Se essa mesma carga de trabalho estiver com uma média de 3.000 IOPS e o tamanho do bloco no cliente estiver definido para 48 KB, os MB/s efetivos para essa carga de trabalho serão 144. Você pode ver que o nó está processando 50% mais dados quando o tamanho do bloco é maior.

Vejam os seguintes exemplos de política de QoS adaptável que tem um tamanho de bloco definido e como os eventos são acionados com base no tamanho do bloco definido no cliente.

Crie uma política e defina a taxa de transferência de pico para 2.500 IOPS/TB com um tamanho de bloco de 32KB. Isso efetivamente define o limite de MB/s para 80 MB/s  $((2500 \text{ IOPS} * 32\text{KB}) / 1000)$  para um volume com 1 TB de capacidade usada. Observe que o Unified Manager gera um evento de aviso quando o valor da taxa de transferência é 10% menor do que o limite definido. Os eventos são gerados nas seguintes situações:

Capacidade utilizada	O evento é gerado quando a taxa de transferência excede este número de ...	
	IOPS	MB/s
1 TB	2.250 IOPS	72 MB/s
2 TB	4.500 IOPS	144 MB/s
5 TB	11.250 IOPS	360 MB/s

Se o volume estiver usando 2TB GB do espaço disponível e o IOPS for 4.000 GB e o tamanho do bloco QoS estiver definido como 32KB GB no cliente, a taxa de transferência MB/s será de 128 MB/s  $((4.000 \text{ IOPS} * 32 \text{ KB}) / 1000)$ . Nenhum evento é gerado neste cenário porque tanto 4.000 IOPS como 128 MB/s estão abaixo do limite para um volume que está usando 2 TB de espaço.

Se o volume estiver usando 2TB GB do espaço disponível e o IOPS for 4.000 GB e o tamanho do bloco QoS estiver definido como 64KB GB no cliente, a taxa de transferência de MB/s será de 256 MB/s  $((4.000 \text{ IOPS} * 64 \text{ KB}) / 1000 \text{ GB})$ . Neste caso, o 4.000 IOPS não gera um evento, mas o valor MB/s de 256 MB/s está acima do limite de 144 MB/s e um evento é gerado.

Por esse motivo, quando um evento é acionado com base em uma violação de MB/s para uma política de QoS adaptável que inclua o tamanho do bloco, um gráfico de MB/s é exibido na seção Diagnóstico do sistema da página Detalhes do evento. Se o evento for acionado com base em uma violação de IOPS para a política de QoS adaptável, um gráfico de IOPS será exibido na seção Diagnóstico do sistema. Se ocorrer uma violação para IOPS e MB/s, você receberá dois eventos.

Para obter mais informações sobre como ajustar as configurações de QoS, "[Visão geral do gerenciamento de desempenho](#)" consulte .

## Resposta a eventos de desempenho superutilizados pelos recursos do nó

O Unified Manager gera recursos de nó eventos de advertência sobreutilizados quando um único nó está operando acima dos limites de sua eficiência operacional e, portanto, potencialmente afetando as latências de workload. Esses eventos definidos pelo sistema oferecem a oportunidade de corrigir possíveis problemas de desempenho antes que muitos workloads sejam afetados pela latência.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Deve haver eventos de desempenho novos ou obsoletos.

O Unified Manager gera eventos de aviso para violações de política de uso excessivo de recursos de nós ao procurar nós que estejam usando mais de 100% da capacidade de performance por mais de 30 minutos.

Você pode usar o Gerenciador de sistema ou os comandos ONTAP para corrigir esse tipo de problema de desempenho, incluindo as seguintes tarefas:

- Criação e aplicação de uma política de QoS a volumes ou LUNs que sobreutilizem recursos do sistema
- Redução do limite máximo de taxa de transferência de QoS de um grupo de políticas ao qual os workloads foram aplicados
- Movendo um workload para um agregado ou nó diferente
- Aumentar a capacidade adicionando discos ao nó ou atualizando para um nó com uma CPU mais rápida e mais RAM

## Passos

1. Exiba a página **Detalhes do evento** para exibir informações sobre o evento.
2. Revise a **Descrição**, que descreve a violação de limite que causou o evento.

Por exemplo, a mensagem "'Perf. O valor de capacidade usada de 139% na simplicity-02 disparou um evento DE AVISO para identificar possíveis problemas de desempenho na unidade Data Processing.'" indica que a capacidade de desempenho no nó simplicity-02 é sobreutilizada e afeta o desempenho do nó.

3. Na seção **Diagnóstico do sistema**, revise os três gráficos: Um para a capacidade de desempenho usada no nó, um para IOPS de armazenamento médio usado pelas principais cargas de trabalho e outro para latência nas principais cargas de trabalho. Quando organizados dessa maneira, você pode ver quais workloads são a causa da latência no nó.

Você pode ver quais workloads têm políticas de QoS aplicadas e quais não, movendo o cursor sobre o gráfico IOPS.

4. Na seção **ações sugeridas**, revise as sugestões e determine quais ações você deve executar para evitar um aumento na latência da carga de trabalho.

Se necessário, clique no botão **Ajuda** para ver mais detalhes sobre as ações sugeridas que você pode executar para tentar resolver o evento de desempenho.

## Resposta a eventos de desempenho de desequilíbrio do cluster

O Unified Manager gera eventos de aviso de desequilíbrio de cluster quando um nó em um cluster está operando com uma carga muito maior do que outros nós e, portanto, potencialmente afetando as latências de workload. Esses eventos definidos pelo sistema oferecem a oportunidade de corrigir possíveis problemas de desempenho antes que muitos workloads sejam afetados pela latência.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

O Unified Manager gera eventos de aviso para violações de políticas de limite de desequilíbrio de cluster comparando o valor de capacidade de desempenho usado para todos os nós do cluster para ver se há uma diferença de carga de 30% entre todos os nós.

Estas etapas ajudam a identificar os recursos a seguir para que você possa mover workloads de alta performance para um nó de utilização mais baixa:

- Os nós no mesmo cluster que são menos utilizados

- Os agregados no novo nó que são os menos utilizados
- Os volumes de maior desempenho no nó atual

## Passos

1. Exiba a página de detalhes do **evento** para exibir informações sobre o evento.
2. Revise a **Descrição**, que descreve a violação de limite que causou o evento.

Por exemplo, a mensagem ""o contador de capacidade de desempenho usado indica uma diferença de carga de 62% entre os nós no cluster Dallas-1-8 e disparou um evento DE AVISO baseado no limite do sistema de 30%"" indica que a capacidade de desempenho em um dos nós está sobreutilizada e afetando o desempenho do nó.

3. Revise o texto em **ações sugeridas** para mover um volume de alto desempenho do nó com o valor de capacidade de alto desempenho usado para um nó com o valor de capacidade de desempenho mais baixo usado.
4. Identifique os nós com o valor mais alto e mais baixo da capacidade de performance usada:
  - a. Na seção **informações do evento**, clique no nome do cluster de origem.
  - b. Na página **Cluster / Performance Summary**, clique em **nodes** na área **Managed Objects**.
  - c. Na página de inventário **nós**, classifique os nós pela coluna **capacidade de desempenho usada**.
  - d. Identifique os nós com o valor mais alto e mais baixo da capacidade de performance usada e anote esses nomes.
5. Identifique o volume usando a maioria das IOPS no nó que tem o valor de capacidade de performance mais alto usado:
  - a. Clique no nó com o valor mais alto de capacidade de desempenho usado.
  - b. Na página **Node / Performance Explorer**, selecione **Admys on this Node** no menu **View and Compare**.
  - c. Clique no agregado com o valor de capacidade de desempenho mais alto usado.
  - d. Na página **Aggregate / Performance Explorer**, selecione **volumes neste agregado** no menu **Exibir e comparar**.
  - e. Classifique os volumes pela coluna **IOPS** e anote o nome do volume usando a maioria das IOPS e o nome do agregado onde o volume reside.
6. Identifique o agregado com a menor utilização no nó que tem o menor valor de capacidade de desempenho usado:
  - a. Clique em **armazenamento > agregados** para exibir a página de inventário **agregados**.
  - b. Selecione a visualização **desempenho: Todos os agregados**.
  - c. Clique no botão **Filter** e adicione um filtro em que ""Node"" é igual ao nome do nó com o menor valor de capacidade de desempenho usado que você anotou na etapa 4.
  - d. Anote o nome do agregado que tem o menor valor de capacidade de desempenho usado.
7. Mova o volume do nó sobrecarregado para o agregado que você identificou como tendo baixa utilização no novo nó.

Você pode executar a operação mover usando o Gerenciador de sistema do ONTAP, os comandos OnCommand Workflow Automation, ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, verifique se você está recebendo o mesmo evento de desequilíbrio de cluster deste cluster.

## Analizando eventos a partir de limites dinâmicos de desempenho

Os eventos gerados a partir de limites dinâmicos indicam que o tempo de resposta (latência) real para uma carga de trabalho é muito alto ou muito baixo, em comparação com o intervalo de tempo de resposta esperado. Você usa a página de detalhes do evento para analisar o evento de desempenho e tomar medidas corretivas, se necessário, para retornar o desempenho ao normal.



Os limites de desempenho dinâmico não são ativados em sistemas Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select.

### Identificação das cargas de trabalho da vítima envolvidas em um evento de desempenho dinâmico

No Unified Manager, você pode identificar quais workloads de volume têm o maior desvio no tempo de resposta (latência) causado por um componente de storage na contenção. Identificar essas cargas de trabalho ajuda você a entender por que os aplicativos clientes que os acessam têm tido um desempenho mais lento do que o normal.

#### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Deve haver eventos de desempenho dinâmico novos, reconhecidos ou obsoletos.

A página de detalhes do evento exibe uma lista das cargas de trabalho definidas pelo usuário e definidas pelo sistema, classificadas pelo maior desvio na atividade ou uso no componente ou mais afetadas pelo evento. Os valores são baseados nos picos identificados pelo Unified Manager quando o evento foi detetado e analisado pela última vez.

#### Passos

1. Exiba a página **Detalhes do evento** para exibir informações sobre o evento.
2. Nos gráficos de latência de workload e atividade de workload, selecione **cargas de trabalho da vítima**.
3. Passe o cursor sobre os gráficos para ver as principais cargas de trabalho definidas pelo usuário que estão afetando o componente e o nome da carga de trabalho da vítima.

### Identificação de workloads bully envolvidos em um evento de performance dinâmico

No Unified Manager, é possível identificar quais workloads têm o maior desvio no uso de um componente de cluster na contenção. A identificação desses workloads ajuda a entender por que certos volumes no cluster têm tempos de resposta (latência) lentos.

#### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Deve haver eventos de desempenho dinâmico novos, reconhecidos ou obsoletos.

A página de detalhes do evento exibe uma lista das cargas de trabalho definidas pelo usuário e definidas pelo sistema classificadas pelo uso mais alto do componente ou mais afetadas pelo evento. Os valores são baseados nos picos identificados pelo Unified Manager quando o evento foi detetado e analisado pela última vez.

#### Passos



1. Exiba a página de detalhes do evento para exibir informações sobre o evento.
2. Nos gráficos latência de workload e atividade de workload, selecione **cargas de trabalho**.
3. Passe o cursor sobre os gráficos para ver as principais cargas de trabalho bully definidas pelo usuário que estão afetando o componente.

### Identificação de cargas de trabalho do SHARK envolvidas em um evento de desempenho dinâmico

No Unified Manager, você pode identificar quais workloads têm o maior desvio no uso de um componente de storage em contenção. A identificação desses workloads ajuda a determinar se esses workloads devem ser movidos para um cluster menos utilizado.

#### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Há um evento dinâmico de desempenho novo, reconhecido ou obsoleto.

A página de detalhes do evento exibe uma lista das cargas de trabalho definidas pelo usuário e definidas pelo sistema classificadas pelo uso mais alto do componente ou mais afetadas pelo evento. Os valores são baseados nos picos identificados pelo Unified Manager quando o evento foi detetado e analisado pela última vez.

#### Passos

1. Exiba a página **Detalhes do evento** para exibir informações sobre o evento.
2. Nos gráficos de latência de workload e atividade de workload, selecione **cargas de trabalho Shark**.
3. Passe o cursor sobre os gráficos para ver as principais cargas de trabalho definidas pelo usuário que estão afetando o componente e o nome da carga de trabalho do SHARK.

### Análise de eventos de performance para uma configuração do MetroCluster

Você pode usar o Unified Manager para analisar um evento de desempenho para uma configuração do MetroCluster. Você pode identificar as cargas de trabalho envolvidas no evento e analisar as ações sugeridas para resolvê-lo.

Os eventos de desempenho do MetroCluster podem ser devido a cargas de trabalho *bully* que estão sobreutilizando os links interswitches (ISLs) entre os clusters ou devido a problemas de integridade do enlace. O Unified Manager monitora cada cluster em uma configuração do MetroCluster de forma independente, sem considerar eventos de desempenho em um cluster de parceiros.

Os eventos de desempenho de ambos os clusters na configuração do MetroCluster também são exibidos na página Painel do Gerenciador Unificado. Você também pode exibir as páginas de integridade do Unified Manager para verificar a integridade de cada cluster e exibir seu relacionamento.

#### Analisando um evento de desempenho dinâmico em um cluster em uma configuração do MetroCluster

Você pode usar o Unified Manager para analisar o cluster em uma configuração do MetroCluster na qual um evento de desempenho foi detetado. Você pode identificar o nome do cluster, o tempo de detecção de eventos e as cargas de trabalho *bully* e *vitima* envolvidas.

#### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Deve haver eventos de desempenho novos, reconhecidos ou obsoletos para uma configuração do MetroCluster.
- Ambos os clusters na configuração do MetroCluster precisam ser monitorados pela mesma instância do Unified Manager.

## Passos

1. Exiba a página **Detalhes do evento** para exibir informações sobre o evento.
2. Revise a descrição do evento para ver os nomes das cargas de trabalho envolvidas e o número de cargas de trabalho envolvidas.

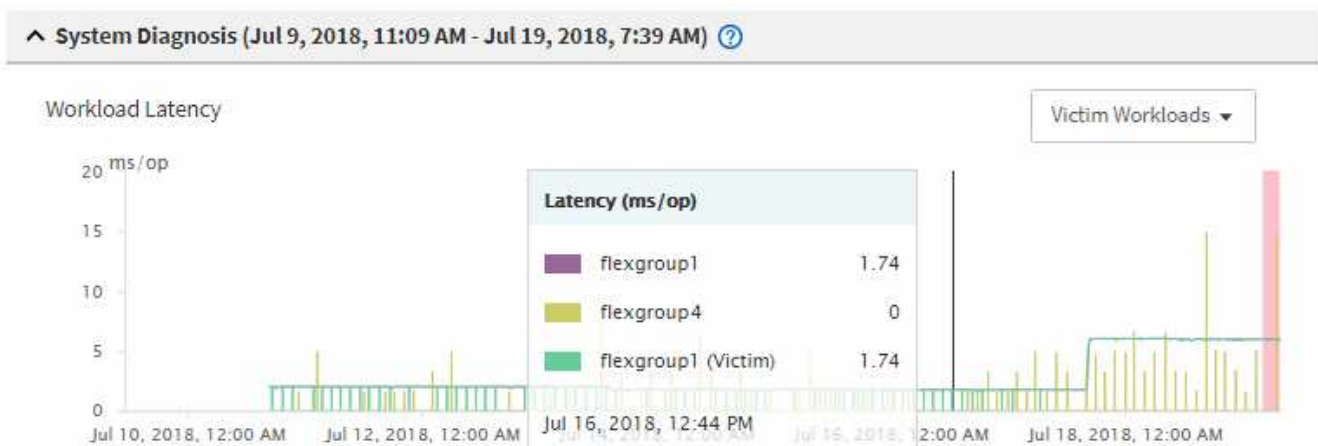
Neste exemplo, o ícone recursos do MetroCluster é vermelho, indicando que os recursos do MetroCluster estão em disputa. Posicione o cursor sobre o ícone para exibir uma descrição do ícone.

Description: 2 victim volumes are slow due to vol\_osv\_siteB2\_5 causing contention on MetroCluster resources



3. Anote o nome do cluster e o tempo de detecção de eventos, que pode ser usado para analisar eventos de desempenho no cluster de parceiros.
4. Nos gráficos, revise as cargas de trabalho *vítima* para confirmar que seus tempos de resposta são maiores do que o limite de desempenho.

Neste exemplo, a carga de trabalho da vítima é exibida no texto do cursor. Os gráficos de latência exibem, em alto nível, um padrão de latência consistente para as cargas de trabalho da vítima envolvidas. Mesmo que a latência anormal das cargas de trabalho da vítima tenha acionado o evento, um padrão de latência consistente pode indicar que as cargas de trabalho estão com desempenho dentro do intervalo esperado, mas que um pico de e/S aumentou a latência e acionou o evento.



Se você instalou recentemente um aplicativo em um cliente que acessa esses workloads de volume e esse aplicativo enviar uma grande quantidade de e/S para eles, talvez você esteja antecipando o aumento das latências. Se a latência das cargas de trabalho retornar dentro do intervalo esperado, o estado do evento muda para obsoleto e permanece nesse estado por mais de 30 minutos, você provavelmente pode ignorar o evento. Se o evento estiver em andamento e permanecer no novo estado, você poderá

investigá-lo ainda mais para determinar se outros problemas causaram o evento.

5. No gráfico de taxa de transferência de carga de trabalho, selecione **Bully cargas de trabalho** para exibir as cargas de trabalho bully.

A presença de cargas de trabalho bully indica que o evento pode ter sido causado por uma ou mais cargas de trabalho no cluster local que sobreutiliza os recursos do MetroCluster. As cargas de trabalho bully têm um alto desvio na taxa de transferência de gravação (MB/s).

Esse gráfico exibe, em alto nível, o padrão de taxa de transferência de gravação (MB/s) para as cargas de trabalho. Você pode revisar o padrão de MB/s de gravação para identificar taxa de transferência anormal, o que pode indicar que uma carga de trabalho está sobreutilizando os recursos do MetroCluster.

Se não houver workloads com bully envolvidos no evento, o evento pode ter sido causado por um problema de integridade com o link entre os clusters ou um problema de desempenho no cluster de parceiros. Você pode usar o Unified Manager para verificar a integridade dos dois clusters em uma configuração do MetroCluster. Você também pode usar o Unified Manager para verificar e analisar eventos de desempenho no cluster de parceiros.

#### **Analisando um evento de desempenho dinâmico para um cluster remoto em uma configuração do MetroCluster**

Você pode usar o Unified Manager para analisar eventos dinâmicos de desempenho em um cluster remoto em uma configuração do MetroCluster. A análise ajuda a determinar se um evento no cluster remoto causou um evento no cluster de parceiros.

#### **Antes de começar**

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter analisado um evento de desempenho em um cluster local em uma configuração do MetroCluster e obtido o tempo de detecção de eventos.
- Você deve ter verificado a integridade do cluster local e do cluster de parceiros envolvidos no evento de desempenho e obtido o nome do cluster de parceiros.

#### **Passos**

1. Faça login na instância do Unified Manager que está monitorando o cluster de parceiros.
2. No painel de navegação esquerdo, clique em **Eventos** para exibir a lista de eventos.
3. No seletor **intervalo de tempo**, selecione **hora anterior** e, em seguida, clique em **aplicar intervalo**.
4. No seletor **Filtering**, selecione **Cluster** no menu suspenso à esquerda, digite o nome do cluster de parceiros no campo de texto e clique em **Apply Filter**.

Se não houver eventos para o cluster selecionado na última hora, isso indica que o cluster não sofreu nenhum problema de desempenho durante o momento em que o evento foi detectado em seu parceiro.

5. Se o cluster selecionado tiver eventos detectados durante a última hora, compare a hora de detecção de eventos com a hora de detecção de eventos para o evento no cluster local.

Se esses eventos envolverem cargas de trabalho bully causando contenção no componente Data Processing, um ou mais desses bullies podem ter causado o evento no cluster local. Você pode clicar no evento para analisá-lo e revisar as ações sugeridas para resolvê-lo na página de detalhes do evento.

Se esses eventos não envolverem cargas de trabalho bully, eles não causarão o evento de desempenho no cluster local.

## Resposta a um evento de desempenho dinâmico causado pela limitação do grupo de políticas de QoS

Você pode usar o Unified Manager para investigar um evento de performance causado por uma política de qualidade do serviço (QoS) que limita a taxa de transferência de workload (MB/s). A regulamentação aumentou os tempos de resposta (latência) das cargas de trabalho de volume no grupo de políticas. Você pode usar as informações do evento para determinar se novos limites nos grupos de políticas são necessários para interromper a limitação.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Deve haver eventos de desempenho novos, reconhecidos ou obsoletos.

### Passos

1. Exiba a página **Detalhes do evento** para exibir informações sobre o evento.
2. Leia a **Descrição**, que exibe o nome das cargas de trabalho afetadas pela limitação.



A descrição pode exibir a mesma carga de trabalho para a vítima e o agressor, porque a limitação torna a carga de trabalho uma vítima de si mesma.

3. Grave o nome do volume usando um aplicativo como um editor de texto.

Você pode pesquisar o nome do volume para localizá-lo mais tarde.

4. Nos gráficos de latência de workload e utilização de carga de trabalho, selecione **Bully workloads**.
5. Passe o cursor sobre os gráficos para ver as principais cargas de trabalho definidas pelo usuário que estão afetando o grupo de políticas.

A carga de trabalho na parte superior da lista tem o desvio mais alto e fez com que a limitação ocorresse. A atividade é a porcentagem do limite do grupo de políticas usado por cada workload.

6. Na área **ações sugeridas**, clique no botão **analisar carga de trabalho** para a carga de trabalho superior.
7. Na página análise de workload, defina o gráfico de latência para exibir todos os componentes de cluster e o gráfico de taxa de transferência para exibir a divisão.

Os gráficos de detalhamento são exibidos sob o gráfico de latência e o gráfico de IOPS.

8. Compare os limites de QoS no gráfico **latência** para ver que quantidade de limitação impactou a latência no momento do evento.

O grupo de políticas de QoS tem uma taxa de transferência máxima de 1.000 operações por segundo (op/seg), que as cargas de trabalho nele não podem exceder coletivamente. No momento do evento, as cargas de trabalho no grupo de políticas tinham uma taxa de transferência combinada de mais de 1.200 op/seg, o que fez com que o grupo de políticas reduzisse sua atividade para 1.000 op/seg


9. Compare os valores de latência **reads/Write** com os valores **reads/Write/Other**.

Ambos os gráficos mostram um alto número de solicitações de leitura com alta latência, mas o número de solicitações e a quantidade de latência para solicitações de gravação são baixos. Esses valores ajudam a determinar se há uma alta quantidade de taxa de transferência ou número de operações que aumentaram a latência. Você pode usar esses valores ao decidir colocar um limite de grupo de políticas na taxa de

transferência ou nas operações.

10. Use o Gerenciador do sistema ONTAP para aumentar o limite atual no grupo de políticas para 1.300 op/seg
11. Após um dia, retorne ao Unified Manager e insira a carga de trabalho que você registrou na Etapa 3 na página **análise de carga de trabalho**.
12. Selecione o gráfico de repartição da taxa de transferência.

É apresentado o gráfico de leituras/gravações/outro.

13. Na parte superior da página, aponte o cursor para o ícone alterar evento (  ) para a alteração de limite do grupo de políticas.
14. Compare o gráfico **reads/Write/Other** com o gráfico **latência**.

As solicitações de leitura e gravação são as mesmas, mas a limitação parou e a latência diminuiu.

### Resposta a um evento de desempenho dinâmico causado por uma falha de disco

Você pode usar o Unified Manager para investigar um evento de performance causado por cargas de trabalho que sobreutilizam um agregado. Você também pode usar o Unified Manager para verificar a integridade do agregado e verificar se eventos recentes de integridade detetados no agregado contribuíram para o evento de desempenho.

#### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Deve haver eventos de desempenho novos, reconhecidos ou obsoletos.

#### Passos

1. Exiba a página **Detalhes do evento** para exibir informações sobre o evento.
2. Leia a **Descrição**, que descreve as cargas de trabalho envolvidas no evento e o componente do cluster em contenção.

Há vários volumes de vítimas cuja latência foi afetada pelo componente do cluster na contenção. O agregado, que está no meio de uma reconstrução RAID para substituir o disco com falha por um disco sobressalente, é o componente de cluster em contenção. Em componente na contenção, o ícone agregado é destacado em vermelho e o nome do agregado é exibido entre parênteses.

3. No gráfico de utilização da carga de trabalho, selecione **Bully workloads**.
4. Passe o cursor sobre o gráfico para ver as principais cargas de trabalho de bully que estão afetando o componente.

As principais cargas de trabalho com maior pico de utilização desde que o evento foi detetado são exibidas na parte superior do gráfico. Uma das principais cargas de trabalho é a integridade do disco da carga de trabalho definida pelo sistema, que indica uma reconstrução RAID. Uma reconstrução é o processo interno envolvido com a reconstrução do agregado com o disco sobressalente. A carga de trabalho de integridade do disco, juntamente com outras cargas de trabalho no agregado, provavelmente causou a contenção no agregado e no evento associado.

5. Depois de confirmar que a atividade da carga de trabalho de integridade do disco causou o evento, aguarde aproximadamente 30 minutos para a conclusão da reconstrução e para que o Unified Manager analise o evento e detete se o agregado ainda está em contenção.

## 6. Atualize os **detalhes do evento**.

Após a conclusão da reconstrução RAID, verifique se o Estado está obsoleto, indicando que o evento foi resolvido.

7. No gráfico de utilização da carga de trabalho, selecione **Bully cargas de trabalho** para visualizar as cargas de trabalho no agregado por utilização máxima.
8. Na área **ações sugeridas**, clique no botão **analisar carga de trabalho** para a carga de trabalho superior.
9. Na página **análise de carga de trabalho**, defina o intervalo de tempo para exibir as últimas 24 horas (1 dia) de dados para o volume selecionado.

Na linha do tempo de eventos, um ponto vermelho (●) indica quando ocorreu o evento de falha de disco.

10. No gráfico de utilização de nó e agregado, oculte a linha para as estatísticas de nó para que apenas a linha agregada permaneça.
11. Compare os dados neste gráfico com os dados no momento do evento no gráfico **latência**.

No momento do evento, a utilização agregada mostra uma grande quantidade de atividade de leitura e gravação, causada pelos processos de reconstrução RAID, o que aumentou a latência do volume selecionado. Algumas horas após o evento, as leituras e as gravações e a latência diminuíram, confirmando que o agregado não está mais na contenção.

## Resposta a um evento de performance dinâmico causado pelo takeover de HA

Você pode usar o Unified Manager para investigar um evento de desempenho causado pela alta Data Processing em um nó de cluster que esteja em um par de alta disponibilidade (HA). Você também pode usar o Unified Manager para verificar a integridade dos nós e verificar se algum evento de integridade recente detetado nos nós contribuiu para o evento de performance.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Deve haver eventos de desempenho novos, reconhecidos ou obsoletos.

### Passos

1. Exiba a página **Detalhes do evento** para exibir informações sobre o evento.
2. Leia a **Descrição**, que descreve as cargas de trabalho envolvidas no evento e o componente do cluster em contenção.

Há um volume de vítima cuja latência foi afetada pelo componente de cluster na contenção. O nó Data Processing, que assumiu todos os workloads de seu nó de parceiro, é o componente do cluster em disputa. Em componente na contenção, o ícone Data Processing é destacado em vermelho e o nome do nó que estava manipulando Data Processing no momento do evento é exibido entre parênteses.

3. Em **Descrição**, clique no nome do volume.

É apresentada a página Explorador de desempenho de volume. Na parte superior da página, na linha hora de Eventos, um ícone de evento de mudança (●) indica a hora em que o Unified Manager detetou o início do takeover de HA.

4. Aponte o cursor para o ícone alterar evento para a aquisição de HA e os detalhes sobre a aquisição de HA serão exibidos no texto do cursor.

No gráfico de latência, um evento indica que o volume selecionado ultrapassou o limite de desempenho devido à alta latência em torno do mesmo tempo que o takeover de HA.

5. Clique em **Zoom View** para exibir o gráfico de latência em uma nova página.
6. No menu Exibir, selecione **componentes de cluster** para exibir a latência total por componente de cluster.
7. Aponte o cursor do Mouse para o ícone alterar evento para o início do controle de HA e compare a latência do Data Processing com a latência total.

No momento do takeover de HA, houve um pico no Data Processing devido à maior demanda de workload no nó Data Processing. O aumento da utilização da CPU aumentou a latência e acionou o evento.

8. Após corrigir o nó com falha, use o Gerenciador de sistema do ONTAP para executar um giveback de HA, que move os workloads do nó do parceiro para o nó fixo.
9. Após a conclusão do HA giveback, após a próxima descoberta de configuração no Unified Manager (aproximadamente 15 minutos), encontre o evento e a carga de trabalho que acionaram o HA OPA na página de inventário **Event Management**.

O evento desencadeado pela aquisição de HA agora tem um estado de obsoleto, o que indica que o evento foi resolvido. A latência no componente Data Processing diminuiu, o que diminuiu a latência total. O nó que o volume selecionado está usando agora para Data Processing resolveu o evento.

## Resolução de eventos de performance

Você pode usar as ações sugeridas para tentar resolver eventos de desempenho por conta própria. As três primeiras sugestões são sempre exibidas, e as ações sob a quarta sugestão são específicas para o tipo de evento exibido.

Os links **Help me do this** fornecem informações adicionais para cada ação sugerida, incluindo instruções para executar uma ação específica. Algumas das ações podem envolver o uso dos comandos do Unified Manager, do ONTAP System Manager, do OnCommand Workflow Automation, da CLI do ONTAP ou uma combinação dessas ferramentas.

### Confirmando que a latência está dentro do intervalo esperado

Quando um componente do cluster está na contenção, os workloads de volume que o usam podem ter reduzido o tempo de resposta (latência). Você pode analisar a latência de cada workload de vítima no componente em contenção para confirmar que sua latência real está dentro do intervalo esperado. Você também pode clicar em um nome de volume para exibir os dados históricos do volume.

Se o evento de desempenho estiver no estado obsoleto, a latência de cada vítima envolvida no evento pode ter retornado dentro do intervalo esperado.

### Analisar o impacto das alterações de configuração na performance do workload

Alterações de configuração no cluster, como um disco com falha, failover de HA ou um volume movido, podem afetar negativamente a performance do volume e causar maior

## latência.

No Unified Manager, você pode revisar a página análise de workload para ver quando ocorreu uma alteração de configuração recente e compará-la com as operações e a latência (tempo de resposta) para ver se houve uma alteração na atividade para o workload de volume selecionado.

As páginas de desempenho do Unified Manager só podem detectar um número limitado de eventos de mudança. As páginas de integridade fornecem alertas para outros eventos causados por alterações de configuração. Você pode pesquisar o volume no Unified Manager para ver o histórico de eventos.

## **Opções para melhorar o desempenho da carga de trabalho do lado do cliente**

Você pode verificar as cargas de trabalho do cliente, como aplicativos ou bancos de dados, que estão enviando e/S para volumes envolvidos em um evento de desempenho para determinar se uma alteração do lado do cliente pode corrigir o evento.

Quando os clientes conectados a volumes em um cluster aumentam suas solicitações de e/S, o cluster precisa trabalhar mais para atender à demanda. Se você souber quais clientes têm um número alto de solicitações de e/S para um volume específico no cluster, poderá melhorar o desempenho do cluster ajustando o número de clientes acessando o volume ou diminuindo a quantidade de e/S para o volume. Você também pode aplicar ou aumentar um limite no grupo de políticas de QoS do qual o volume é membro.

Você pode investigar clientes e seus aplicativos para determinar se os clientes estão enviando mais e/S do que o normal, o que pode estar causando contenção em um componente de cluster. Na página de detalhes do evento, a seção Diagnóstico do sistema exibe as cargas de trabalho de volume superior usando o componente em contenção. Se você sabe qual cliente está acessando um volume específico, você pode ir para o cliente para determinar se o hardware do cliente ou um aplicativo não está operando como esperado ou está fazendo mais trabalho do que o habitual.

Em uma configuração do MetroCluster, as solicitações de gravação em um volume em um cluster local são espelhadas em um volume no cluster remoto. Manter o volume de origem no cluster local sincronizado com o volume de destino no cluster remoto também pode aumentar a demanda dos dois clusters na configuração do MetroCluster. Com a redução das solicitações de gravação para esses volumes espelhados, os clusters realizam menos operações de sincronização, o que reduz o impacto na performance em outros workloads.

## **Verifique se há problemas de cliente ou rede**

Quando os clientes conectados a volumes em um cluster aumentam suas solicitações de e/S, o cluster precisa trabalhar mais para atender à demanda. O aumento da demanda no cluster pode colocar um componente na contenção, aumentar a latência dos workloads que o usam e acionar um evento no Unified Manager.

Na página de detalhes do evento, a seção Diagnóstico do sistema exibe as cargas de trabalho de volume superior usando o componente em contenção. Se você sabe qual cliente está acessando um volume específico, você pode ir para o cliente para determinar se o hardware do cliente ou um aplicativo não está operando como esperado ou está fazendo mais trabalho do que o habitual. Poderá ser necessário contactar o administrador do cliente ou o fornecedor da aplicação para obter assistência.

Você pode verificar sua infraestrutura de rede para determinar se há problemas de hardware, gargalos ou cargas de trabalho concorrentes que podem ter causado solicitações de e/S entre o cluster e os clientes conectados a um desempenho mais lento do que o esperado. Poderá ser necessário contactar o administrador da rede para obter assistência.



## Verifique se outros volumes no grupo de políticas de QoS têm atividade excepcionalmente alta

Você pode analisar os workloads no grupo de políticas de qualidade do serviço (QoS) que tem a alteração mais alta na atividade para determinar se mais de um workload causou o evento. Você também pode ver se outros workloads ainda estão excedendo o limite de taxa de transferência definido ou se eles estão de volta ao intervalo de atividade esperado.

Na página de detalhes do evento, na seção Diagnóstico do sistema, você pode classificar as cargas de trabalho por desvio de pico na atividade para exibir as cargas de trabalho com a alteração mais alta na atividade na parte superior da tabela. Essas cargas de trabalho podem ser os "bullies" cuja atividade excedeu o limite definido e pode ter causado o evento.

É possível navegar até a página análise de workload de workload de volume para analisar a atividade de IOPS. Se a carga de trabalho tiver períodos de atividade de operações muito altas, ela pode ter contribuído para o evento. Você pode alterar as configurações do grupo de políticas para a carga de trabalho ou mover a carga de trabalho para um grupo de políticas diferente.


Você pode usar o Gerenciador de sistema do ONTAP ou os comandos CLI do ONTAP para gerenciar grupos de políticas, como a seguir:

- Crie um grupo de políticas.
- Adicione ou remova cargas de trabalho em um grupo de políticas.
- Mover uma carga de trabalho entre grupos de políticas.
- Altere o limite de taxa de transferência de um grupo de políticas.

## Mover interfaces lógicas (LIFs)

Mover interfaces lógicas (LIFs) para uma porta menos ocupada pode ajudar a melhorar o balanceamento de carga, auxiliar nas operações de manutenção e ajuste de desempenho e reduzir o acesso indireto.

O acesso indireto pode reduzir a eficiência do sistema. Isso ocorre quando uma carga de trabalho de volume está usando nós diferentes para processamento de rede e Data Processing. Para reduzir o acesso indireto, você pode reorganizar LIFs, o que envolve mover LIFs para usar o mesmo nó para processamento de rede e Data Processing. Você pode configurar o balanceamento de carga para que o ONTAP mova automaticamente LIFs ocupadas para uma porta diferente ou você pode mover um LIF manualmente.

Benefícios	Considerações
<ul style="list-style-type: none"><li>• Melhorar o balanceamento de carga.</li><li>• Reduzir o acesso indireto.</li></ul>	 <p>Ao mover um LIF conectado a compartilhamentos CIFS, os clientes que acessam os compartilhamentos CIFS são desconectados. Quaisquer solicitações de leitura ou gravação para os compartilhamentos CIFS são interrompidas.</p>

Você usa os comandos ONTAP para configurar o balanceamento de carga. Para obter mais informações,

consulte a documentação de rede do ONTAP.

Você usa o Gerenciador de sistema do ONTAP e os comandos CLI do ONTAP para mover LIFs manualmente.

## **Execute operações de eficiência de storage em momentos menos ocupados**

Você pode modificar a política ou a programação que lida com operações de eficiência de storage para execução quando os workloads de volume afetados estiverem menos ocupados.

As operações de eficiência de storage podem usar uma grande quantidade de recursos de CPU do cluster e se tornar um bully para os volumes em que as operações estão sendo executadas. Se os volumes das vítimas tiverem alta atividade ao mesmo tempo em que as operações de eficiência de storage são executadas, sua latência poderá aumentar e acionar um evento.

Na página de detalhes do evento, a seção Diagnóstico do sistema exibe cargas de trabalho no grupo de políticas de QoS por desvio de pico na atividade para identificar as cargas de trabalho bully. Se você vir "eficiência de toragem" exibida perto da parte superior da tabela, essas operações estão intimidando as cargas de trabalho da vítima. Ao modificar a política de eficiência ou a programação para execução quando esses workloads estão menos ocupados, é possível evitar que as operações de eficiência de storage causem contenção em um cluster.

Você pode usar o Gerenciador de sistemas do ONTAP para gerenciar políticas de eficiência. Você pode usar os comandos ONTAP para gerenciar políticas e programações de eficiência.

### **Qual é a eficiência de storage**

A eficiência de storage permite armazenar a quantidade máxima de dados pelo menor custo possível, além de acomodar o crescimento rápido dos dados e consumir menos espaço. A estratégia da NetApp para eficiência de storage é baseada na base incorporada da virtualização de storage e no storage unificado fornecida pelo sistema operacional ONTAP central e pelo sistema de arquivos Write Anywhere File Layout (WAFL).

A eficiência de storage inclui o uso de tecnologias como thin Provisioning, cópia Snapshot, deduplicação, compressão de dados, FlexClone, thin replication com SnapVault e volume SnapMirror, RAID-DP, Flash Cache, agregado de Flash Pool e agregados habilitados para FabricPool, que ajudam a aumentar a utilização do storage e a diminuir os custos de storage.

A arquitetura de storage unificada permite consolidar com eficiência uma rede de área de storage (SAN), armazenamento conectado à rede (nas) e storage secundário em uma única plataforma.

Unidades de disco de alta densidade, como unidades SATA (serial Advanced Technology Attachment) configuradas no Flash Pool Aggregate ou com Flash Cache e tecnologia RAID-DP, aumentam a eficiência sem afetar o desempenho e a resiliência.

Um agregado habilitado para FabricPool inclui um agregado totalmente SSD ou agregado de HDD (começando com ONTAP 9.8) como a camada de desempenho local e um armazenamento de objetos que você especificar como a camada de nuvem. A configuração do FabricPool ajuda você a gerenciar qual camada de storage (a camada local ou a camada de nuvem) os dados devem ser armazenados com base no fato de que eles são acessados com frequência.

Tecnologias como thin Provisioning, cópia Snapshot, deduplicação, compressão de dados, thin replication com

SnapVault e volume SnapMirror e FlexClone oferecem uma economia melhor. Você pode usar essas tecnologias individualmente ou em conjunto para obter a máxima eficiência de storage.

## Adicionar discos e realocar dados

Você pode adicionar discos a um agregado para aumentar a capacidade de storage e o desempenho desse agregado. Depois de adicionar os discos, você verá uma melhoria no desempenho de leitura somente depois de realocá-los entre os discos adicionados.

Use estas instruções quando o Unified Manager receber eventos agregados acionados por limites dinâmicos ou por limites de performance definidos pelo sistema:

- Quando você recebeu um evento de limite dinâmico, na página de detalhes do evento, o ícone do componente do cluster que representa o agregado na contenção é realçado em vermelho.

Abaixo do ícone, entre parênteses, está o nome do agregado, que identifica o agregado ao qual você pode adicionar discos.

- Quando você recebeu um evento de limite definido pelo sistema, na página de detalhes do evento, o texto de descrição do evento lista o nome do agregado que está tendo o problema.

Você pode adicionar discos e realocar dados nesse agregado.

Os discos adicionados ao agregado já devem existir no cluster. Se o cluster não tiver discos extras disponíveis, talvez seja necessário entrar em Contato com o administrador ou comprar mais discos. Você pode usar o Gerenciador de sistema do ONTAP ou os comandos ONTAP para adicionar discos a um agregado.



Você deve realocar dados somente ao usar agregados HDD e Flash Pool. Não realocar dados em agregados SSD ou FabricPool.

## Como habilitar o Flash Cache em um nó pode melhorar a performance do workload

Você pode melhorar o desempenho da carga de trabalho habilitando o armazenamento em cache inteligente de dados Flash Cache em cada nó do cluster.

Um módulo Flash Cache, ou módulo de memória baseado em PCIe do módulo de aceleração de desempenho, otimiza o desempenho de cargas de trabalho aleatórias com uso intensivo de leitura, funcionando como um cache de leitura externo inteligente. Este hardware funciona em conjunto com o componente de software cache externo WAFL do ONTAP.

No Unified Manager, na página de detalhes do evento, o ícone do componente do cluster que representa o agregado na contenção é realçado em vermelho. Abaixo do ícone, entre parênteses, está o nome do agregado, que identifica o agregado. Você pode habilitar o Flash Cache no nó no qual o agregado reside.

Você pode usar o Gerenciador de sistema do ONTAP ou os comandos ONTAP para ver se o Flash Cache está instalado ou ativado e ativá-lo se ainda não estiver habilitado. O comando a seguir indica se o Flash Cache está habilitado em um nó específico: `cluster::> run local options flexscale.enable`

Para obter mais informações sobre o Flash Cache e os requisitos para usá-lo, consulte o seguinte relatório técnico:

["Relatório técnico 3832: Guia de práticas recomendadas do Flash Cache"](#)

## Como habilitar o Flash Pool em um agregado de storage pode melhorar o desempenho do workload

Você pode melhorar o desempenho do workload habilitando o recurso Flash Pool em um agregado. Um Flash Pool é um agregado que incorpora HDDs e SSDs. Os HDDs são usados para storage primário e os SSDs fornecem um cache de leitura e gravação de alta performance para aumentar o desempenho agregado.

No Unified Manager, a página de detalhes do evento exibe o nome do agregado em contenção. Você pode usar o Gerenciador de sistema do ONTAP ou os comandos ONTAP para ver se o Flash Pool está habilitado para um agregado. Se você tiver SSDs instalados, você pode usar a interface de linha de comando para ativá-la. Se você tiver SSDs instalados, poderá executar o seguinte comando no agregado para ver se o Flash Pool está habilitado: `cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled`

Neste comando `aggr_name`, é o nome do agregado, como o agregado na contenção.

Para obter mais informações sobre o Flash Pool e os requisitos para usá-lo, consulte o *Clustered Data ONTAP Physical Storage Management Guide*.

## Verificação da integridade da configuração do MetroCluster

Use o Unified Manager para analisar a integridade dos clusters em uma configuração do MetroCluster por IP ou FC. Os eventos e o status de integridade ajudam a determinar se há problemas de hardware ou software que podem estar afetando a performance dos workloads.

Se você configurar o Unified Manager para enviar alertas por e-mail, poderá verificar se há problemas de integridade no cluster local ou remoto que possam ter contribuído para um evento de desempenho. Na GUI do Unified Manager, você pode selecionar **Gerenciamento de eventos** para ver uma lista de eventos atuais e usar os filtros para exibir apenas eventos de configuração do MetroCluster.

Para obter mais informações, consulte ["Verificação da integridade dos clusters em uma configuração do MetroCluster"](#)

## Verificação da configuração do MetroCluster

Você pode evitar problemas de performance de workloads espelhados em configurações MetroCluster em FC e IP garantindo que a configuração MetroCluster esteja configurada corretamente. Você também pode melhorar a performance do workload alterando a configuração ou atualizando componentes de software ou hardware.

Consulte a ["Documentação do MetroCluster"](#) para obter instruções sobre como configurar os clusters na configuração MetroCluster, incluindo os switches Fibre Channel (FC), cabos e ISLs (links entre switches). Ele também ajuda a configurar o software MetroCluster para que os clusters locais e remotos possam se comunicar com dados de volume espelhado. Para obter informações específicas sobre a configuração do MetroCluster sobre IP, ["Instale uma configuração IP do MetroCluster"](#) consulte .

Você pode comparar a configuração do MetroCluster com os requisitos do ["Documentação do MetroCluster"](#) para determinar se a alteração ou atualização de componentes na configuração do MetroCluster pode melhorar a performance do workload. Esta comparação pode ajudá-lo a responder às seguintes perguntas:

- Os controladores são apropriados para seus workloads?
- Você precisa atualizar seus pacotes ISL para uma largura de banda maior para lidar com mais throughput?
- Você pode ajustar os créditos buffer-to-buffer (BBC) em seus switches para aumentar a largura de banda?
- Se seus workloads tiverem taxa de transferência de gravação alta no storage de unidade de estado sólido (SSD), você precisará atualizar suas pontes FC para SAS para acomodar a taxa de transferência?

### Informações relacionadas

- Para obter informações sobre como substituir ou atualizar componentes do MetroCluster, consulte ["Documentação do MetroCluster"](#).
- Para obter informações sobre como atualizar controladores, ["Atualização de controladores em uma configuração MetroCluster FC usando switchover e switchback"](#) consulte e. ["Atualização de controladores em uma configuração MetroCluster IP usando switchover e switchback"](#)

## Movimentação de workloads para um agregado diferente

Use o Unified Manager para ajudar a identificar um agregado que está menos ocupado do que o agregado onde seus workloads atualmente residem e, em seguida, você pode mover volumes selecionados ou LUNs para esse agregado. Mover workloads de alta performance para um agregado menos ocupado ou um agregado com storage flash ativado permite que o workload execute com mais eficiência.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter registrado o nome do agregado que está tendo um problema de desempenho no momento.
- Você deve ter registrado a data e a hora em que o agregado recebeu o evento.
- O Unified Manager precisa ter coletado e analisado um mês ou mais dos dados de desempenho.

Essas etapas ajudam a identificar os recursos a seguir para que você possa mover workloads de alta performance para um agregado de menor utilização:

- Os agregados no mesmo cluster que são menos utilizados
- Os volumes de maior desempenho no agregado atual

### Passos

1. Identifique o agregado no cluster que é o menos utilizado:

- a. Na página de detalhes do **evento**, clique no nome do cluster no qual o agregado reside.

Os detalhes do cluster são exibidos na página Performance/Cluster Landing.

- b. Na página **Resumo**, clique em **agregados** no painel **objetos gerenciados**.

A lista de agregados neste cluster é exibida.

- c. Clique na coluna **utilização** para classificar os agregados pelo menos utilizado.

Você também pode identificar aqueles agregados que têm a maior capacidade **Free**. Isso fornece uma lista de agregados potenciais aos quais você pode querer mover workloads.

d. Anote o nome do agregado para o qual você deseja mover as cargas de trabalho.

2. Identifique os volumes de alto desempenho do agregado que recebeu o evento:

a. Clique no agregado que está tendo o problema de desempenho.

Os detalhes agregados são exibidos na página Explorador de desempenho/agregado.

b. No seletor **intervalo de tempo**, selecione **últimos 30 dias** e, em seguida, clique em **aplicar intervalo**.

Isso permite que você visualize um período de histórico de desempenho mais longo do que o padrão de 72 horas. Você quer mover um volume que esteja usando muitos recursos de forma consistente, não apenas nas últimas 72 horas.

c. No controle **Exibir e comparar**, selecione **volumes neste agregado**.

Uma lista de volumes FlexVol e volumes constituintes FlexGroup neste agregado é exibida.

d. Classifique os volumes por MB/s mais altos e, em seguida, por IOPS mais alto, para ver os volumes com melhor desempenho.

e. Anote os nomes dos volumes que você deseja mover para um agregado diferente.

3. Mova os volumes de alto desempenho para o agregado que você identificou como tendo baixa utilização.

Você pode executar a operação mover usando o Gerenciador de sistema do ONTAP, os comandos OnCommand Workflow Automation, ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, verifique se você está recebendo o mesmo tipo de eventos desse nó ou agregado.

## Movimentação de workloads para um nó diferente

Você pode usar o Unified Manager para ajudar a identificar um agregado em um nó diferente que esteja menos ocupado do que o nó no qual seus workloads estão em execução no momento e, em seguida, mover volumes selecionados para esse agregado. Mover workloads de alta performance para um agregado em um nó menos ocupado permite que as cargas de trabalho em ambos os nós tenham desempenho mais eficiente.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter registrado o nome do nó que está tendo um problema de desempenho no momento.
- Você precisa ter registrado a data e a hora em que o nó recebeu o evento de performance.
- O Unified Manager precisa ter coletado e analisado os dados de desempenho por um mês ou mais.

Esse procedimento ajuda você a identificar os recursos a seguir para mover workloads de alta performance para um nó mais utilizado:

- Os nós no mesmo cluster que têm a maior capacidade de performance gratuita
- Agregados no novo nó que têm a maior capacidade de performance livre
- Os volumes de maior desempenho no nó atual

### Passos

1. Identifique um nó no cluster que tenha a maior capacidade de desempenho livre:
  - a. Na página **Detalhes do evento**, clique no nome do cluster no qual o nó reside.

Os detalhes do cluster são exibidos na página Performance/Cluster Landing.
  - b. Na guia **Summary**, clique em **nodes** no painel **Managed Objects**.

A lista de nós neste cluster é exibida.
  - c. Clique na coluna **capacidade de desempenho usada** para classificar os nós pelo menos percentual usado.

Isso fornece uma lista de nós potenciais para os quais você pode querer mover cargas de trabalho.
  - d. Anote o nome do nó para o qual você deseja mover as cargas de trabalho.
2. Identifique um agregado no novo nó que seja o menos utilizado:
  - a. No painel de navegação à esquerda, clique em **Storage > Aggregates** e selecione **Performance > All agreements** (desempenho\* > todos os agregados\*) no menu View (Visualizar).

A visualização desempenho: Todos os agregados é exibida.
  - b. Clique em **Filtering**, selecione **Node** no menu suspenso à esquerda, digite o nome do nó no campo de texto e clique em **Apply Filter**.

A visualização desempenho: Todos os agregados é reexibida com a lista de agregados disponíveis neste nó.
  - c. Clique na coluna **capacidade de desempenho usada** para classificar os agregados pelo menos usado.

Isso fornece uma lista de agregados potenciais aos quais você pode querer mover workloads.
  - d. Anote o nome do agregado para o qual você deseja mover as cargas de trabalho.
3. Identifique os workloads de alta performance do nó que recebeu o evento:
  - a. Retornar à página **Detalhes do evento** para o evento.
  - b. No campo **volumes afetados**, clique no link para o número de volumes.

A exibição desempenho: Todos os volumes é exibida com uma lista filtrada dos volumes nesse nó.
  - c. Clique na coluna **capacidade total** para classificar os volumes pelo maior espaço alocado.

Isso fornece uma lista de volumes potenciais que você pode querer mover.
  - d. Anote os nomes dos volumes que você deseja mover e os nomes dos agregados atuais nos quais eles residem.
4. Mova os volumes para os agregados que você identificou como tendo a maior capacidade de performance livre no novo nó.

Você pode executar a operação mover usando o Gerenciador de sistema do ONTAP, os comandos OnCommand Workflow Automation, ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, você pode verificar se está recebendo o mesmo tipo de eventos desse nó ou agregado.

## Movimentação de workloads para um agregado em um nó diferente

Você pode usar o Unified Manager para ajudar a identificar um agregado em um nó diferente que esteja menos ocupado do que o nó em que seus workloads estão atualmente em execução e, em seguida, mover volumes selecionados para esse agregado. Mover workloads de alta performance para um agregado em um nó menos ocupado permite que as cargas de trabalho em ambos os nós tenham desempenho mais eficiente.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter registrado o nome do nó que está tendo um problema de desempenho no momento.
- Você precisa ter registrado a data e a hora em que o nó recebeu o evento de performance.
- O Unified Manager precisa ter coletado e analisado um mês ou mais dos dados de desempenho.

Estas etapas ajudam a identificar os recursos a seguir para que você possa mover workloads de alta performance para um nó de utilização mais baixa:

- Os nós no mesmo cluster que são menos utilizados
- Os agregados no novo nó que são os menos utilizados
- Os volumes de maior desempenho no nó atual

### Passos

1. Identifique um nó no cluster que seja o menos utilizado:

- a. Na página de detalhes do **evento**, clique no nome do cluster no qual o nó reside.

Os detalhes do cluster são exibidos na página Performance/Cluster Landing.

- b. Na página **Summary**, clique em **nodes** no painel **Managed Objects**.

A lista de nós neste cluster é exibida.

- c. Clique na coluna **utilização** para classificar os nós pelo menos utilizado.

Você também pode identificar os nós que têm a maior capacidade **Free**. Isso fornece uma lista de nós potenciais para os quais você pode querer mover cargas de trabalho.

- d. Anote o nome do nó para o qual você deseja mover as cargas de trabalho.

2. Identifique um agregado no novo nó que seja o menos utilizado:

- a. No painel de navegação à esquerda, clique em **Storage > Aggregates** e selecione **Performance > All agreements** (desempenho\* > todos os agregados\*) no menu View (Visualizar).

A visualização desempenho: Todos os agregados é exibida.

- b. Clique em **Filtering**, selecione **Node** no menu suspenso à esquerda, digite o nome do nó no campo de texto e clique em **Apply Filter**.

A visualização desempenho: Todos os agregados é reexibida com a lista de agregados disponíveis neste nó.



c. Clique na coluna **utilização** para classificar os agregados pelo menos utilizado.

Você também pode identificar aqueles agregados que têm a maior capacidade **Free**. Isso fornece uma lista de agregados potenciais aos quais você pode querer mover workloads.

d. Anote o nome do agregado para o qual você deseja mover as cargas de trabalho.

3. Identifique os workloads de alta performance do nó que recebeu o evento:

a. Voltar à página de detalhes do **evento** para o evento.

b. No campo **volumes afetados**, clique no link para o número de volumes.

A exibição desempenho: Todos os volumes é exibida com uma lista filtrada dos volumes nesse nó.

c. Clique na coluna **capacidade total** para classificar os volumes pelo maior espaço alocado.

Isso fornece uma lista de volumes potenciais que você pode querer mover.

d. Anote os nomes dos volumes que você deseja mover e os nomes dos agregados atuais nos quais eles residem.

4. Mova os volumes para os agregados identificados como tendo baixa utilização no novo nó.

Você pode executar a operação mover usando o Gerenciador de sistema do ONTAP, os comandos OnCommand Workflow Automation, ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, verifique se você está recebendo o mesmo tipo de eventos desse nó ou agregado.

## Movimentação de workloads para um nó em um par de HA diferente

Use o Unified Manager para ajudar a identificar um agregado em um nó em um par de alta disponibilidade (HA) diferente que tenha mais capacidade de performance livre do que o par de HA em que seus workloads estão em execução no momento. Depois, você pode mover volumes selecionados para agregados no novo par de HA.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- O cluster precisa consistir em, no mínimo, dois pares de HA

Você não pode usar esse processo de correção se tiver apenas um par de HA no cluster.

- Você precisa ter registrado os nomes dos dois nós no par de HA que estão tendo problemas de performance no momento.
- Você precisa ter registrado a data e a hora em que os nós receberam o evento de performance.
- O Unified Manager precisa ter coletado e analisado os dados de desempenho por um mês ou mais.

Mover workloads de alta performance para um agregado em um nó com mais capacidade de performance gratuita permite que os workloads em ambos os nós tenham performance mais eficiente. Esse procedimento ajuda você a identificar os recursos a seguir para mover workloads de alta performance para um nó que tenha mais capacidade de performance livre em um par de HA diferente:

- Os nós de um par de HA diferente no mesmo cluster que têm a maior capacidade de performance gratuita

- Agregados nos novos nós que têm a maior capacidade de performance livre
- Os volumes com melhor desempenho nos nós atuais

## Passos

1. Identifique os nós que fazem parte de um par de HA diferente no mesmo cluster:
  - a. Na página **Detalhes do evento**, clique no nome do cluster no qual os nós residem.  
  
Os detalhes do cluster são exibidos na página Performance/Cluster Landing.
  - b. Na página **Summary**, clique em **nodes** no painel **Managed Objects**.  
  
A lista de nós neste cluster é exibida na visualização desempenho: Todos os nós.
  - c. Anote os nomes dos nós que estão em diferentes pares de HA do par de HA que está tendo problemas de performance no momento.
2. Identifique um nó no novo par de HA que tenha a maior capacidade de performance gratuita:
  - a. Na exibição **desempenho: Todos os nós**, clique na coluna **capacidade de desempenho usada** para classificar os nós pela menor porcentagem usada.  
  
Isso fornece uma lista de nós potenciais para os quais você pode querer mover cargas de trabalho.
  - b. Anote o nome do nó em um par de HA diferente para o qual você deseja mover os workloads.
3. Identifique um agregado no novo nó que tenha a maior capacidade de desempenho livre:
  - a. Na visualização **Performance: All Nodes** (desempenho: Todos os nós\*), clique no nó.  
  
Os detalhes do nó são exibidos na página Performance/Node Explorer.
  - b. No menu **Exibir e comparar**, selecione **agregados neste nó**.  
  
Os agregados neste nó são exibidos na grade.
  - c. Clique na coluna **capacidade de desempenho usada** para classificar os agregados pelo menos usado.  
  
Isso fornece uma lista de agregados potenciais aos quais você pode querer mover workloads.
  - d. Anote o nome do agregado para o qual você deseja mover as cargas de trabalho.
4. Identifique os workloads de alta performance dos nós que receberam o evento:
  - a. Voltar à página de detalhes do **evento** para o evento.
  - b. No campo **volumes afetados**, clique no link para o número de volumes do primeiro nó.  
  
A exibição desempenho: Todos os volumes é exibida com uma lista filtrada dos volumes nesse nó.
  - c. Clique na coluna **capacidade total** para classificar os volumes pelo maior espaço alocado.  
  
Isso fornece uma lista de volumes potenciais que você pode querer mover.
  - d. Anote os nomes dos volumes que você deseja mover e os nomes dos agregados atuais nos quais eles residem.
  - e. Execute as etapas 4c e 4D para o segundo nó que fez parte desse evento para identificar possíveis volumes que você deseja mover desse nó também.

5. Mova os volumes para os agregados que você identificou como tendo a maior capacidade de performance livre no novo nó.

Você pode executar a operação mover usando o Gerenciador de sistema do ONTAP, os comandos OnCommand Workflow Automation, ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, você pode verificar se está recebendo o mesmo tipo de eventos desse nó ou agregado.

## Movimentação de workloads para outro nó em um par de HA diferente

Use o Unified Manager para ajudar a identificar um agregado em um nó em um par de HA diferente que esteja menos ocupado do que o par de HA em que seus workloads estão em execução no momento. Depois, você pode mover volumes selecionados para agregados no novo par de HA. Mover workloads de alta performance para um agregado em um nó menos ocupado permite que as cargas de trabalho em ambos os nós tenham desempenho mais eficiente.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- O cluster precisa consistir em, no mínimo, dois pares de HA. Você não pode usar esse processo de correção se tiver apenas um par de HA no cluster.
- Você precisa ter registrado os nomes dos dois nós no par de HA que estão tendo o problema de performance no momento.
- Você precisa ter registrado a data e a hora em que os nós receberam o evento de performance.
- O Unified Manager precisa ter coletado e analisado um mês ou mais dos dados de desempenho.

Estas etapas ajudam a identificar os recursos a seguir para que você possa mover workloads de alta performance para um nó mais utilizado em um par de HA diferente:

- Os nós de um par de HA diferente no mesmo cluster que são menos utilizados
- Os agregados nos novos nós que são os menos utilizados
- Os volumes com melhor desempenho nos nós atuais

### Passos

1. Identifique os nós que fazem parte de um par de HA diferente no mesmo cluster:
  - a. No painel de navegação esquerdo, clique em **Storage > clusters** e selecione **Performance > All clusters** no menu Exibir.  
  
A visualização desempenho: Todos os clusters é exibida.
  - b. Clique no número no campo **contagem de nós** para o cluster atual.  
  
A visualização desempenho: Todos os nós é exibida.
  - c. Anote os nomes dos nós que estão em diferentes pares de HA do par de HA que está tendo o problema de performance no momento.
2. Identifique um nó no novo par de HA que seja o menos utilizado:
  - a. Clique na coluna **utilização** para classificar os nós pelo menos utilizado.

Você também pode identificar os nós que têm a maior capacidade **Free**. Isso fornece uma lista de nós potenciais para os quais você pode querer mover cargas de trabalho.

b. Anote o nome do nó para o qual você deseja mover as cargas de trabalho.

3. Identifique um agregado no novo nó que seja o menos utilizado:

a. No painel de navegação à esquerda, clique em **Storage > Aggregates** e selecione **Performance > All agreements** (desempenho\* > todos os agregados\*) no menu View (Visualizar).

A visualização desempenho: Todos os agregados é exibida.

b. Clique em **Filtering**, selecione **Node** no menu suspenso à esquerda, digite o nome do nó no campo de texto e clique em **Apply Filter**.

A visualização desempenho: Todos os agregados é reexibida com a lista de agregados disponíveis neste nó.

c. Clique na coluna **utilização** para classificar os agregados pelo menos utilizado.

Você também pode identificar aqueles agregados que têm a maior capacidade **Free**. Isso fornece uma lista de agregados potenciais aos quais você pode querer mover workloads.

d. Anote o nome do agregado para o qual você deseja mover as cargas de trabalho.

4. Identifique os workloads de alta performance dos nós que receberam o evento:

a. Voltar à página de detalhes do **evento** para o evento.

b. No campo **volumes afetados**, clique no link para o número de volumes do primeiro nó.

A exibição desempenho: Todos os volumes é exibida com uma lista filtrada dos volumes nesse nó.

c. Clique na coluna **capacidade total** para classificar os volumes pelo maior espaço alocado.

Isso fornece uma lista de volumes potenciais que você pode querer mover.

d. Anote os nomes dos volumes que você deseja mover e os nomes dos agregados atuais nos quais eles residem.

e. Execute as etapas 4c e 4D para o segundo nó que fez parte desse evento para identificar possíveis volumes que você deseja mover desse nó também.

5. Mova os volumes para os agregados identificados como tendo baixa utilização no novo nó.

Você pode executar a operação mover usando o Gerenciador de sistema do ONTAP, os comandos OnCommand Workflow Automation, ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, verifique se você está recebendo o mesmo tipo de eventos desse nó ou agregado.

## Use as configurações de política de QoS para priorizar o trabalho nesse nó

Você pode definir um limite em um grupo de políticas de QoS para controlar o limite de taxa de transferência de e/S por segundo (IOPS) ou Mbps para os workloads nele contidos. Se as cargas de trabalho estiverem em um grupo de políticas sem limite definido, como o grupo de políticas padrão ou o limite definido não atender às suas necessidades, você poderá aumentar o limite definido ou mover as cargas de trabalho

para um grupo de políticas novo ou existente que tenha o limite desejado.

Se um evento de desempenho em um nó for causado por cargas de trabalho que usam os recursos do nó, a descrição do evento na página de detalhes do evento exibirá um link para a lista de volumes envolvidos. Na página desempenho/volumes, você pode classificar os volumes afetados por IOPS e Mbps para ver quais workloads têm o uso mais alto que pode ter contribuído para o evento.

Ao atribuir os volumes que estão sobreusando os recursos do nó a uma configuração de grupo de políticas mais restritiva, o grupo de políticas mantém as cargas de trabalho para restringir sua atividade, o que pode reduzir o uso dos recursos nesse nó.

Você pode usar o Gerenciador de sistema do ONTAP ou os comandos ONTAP para gerenciar grupos de políticas, incluindo as seguintes tarefas:

- Criando um grupo de políticas
- Adição ou remoção de cargas de trabalho em um grupo de políticas
- Movimentação de uma carga de trabalho entre grupos de políticas
- Alterar o limite de taxa de transferência de um grupo de políticas

## Remover volumes inativos e LUNs

Quando o espaço livre agregado for identificado como um problema, você poderá pesquisar volumes e LUNs não utilizados e excluí-los do agregado. Isso pode ajudar a aliviar o problema de pouco espaço em disco.

Se um evento de performance em um agregado for causado por pouco espaço em disco, há algumas maneiras de determinar quais volumes e LUNs não estão mais sendo usados.

Para identificar volumes não utilizados:

- Na página Detalhes do evento, o campo **contagem de objetos afetados** fornece um link que exibe a lista de volumes afetados.

Clique no link para exibir os volumes na exibição desempenho: Todos os volumes. A partir daí, você pode classificar os volumes afetados por **IOPS** para ver quais volumes não estiveram ativos.

Para identificar LUNs não utilizados:

1. Na página de detalhes do evento, anote o nome do agregado no qual o evento ocorreu.
2. No painel de navegação esquerdo, clique em **armazenamento > LUNs** e selecione **desempenho > todos os LUNs** no menu Exibir.
3. Clique em **Filtering**, selecione **Aggregate** no menu suspenso à esquerda, digite o nome do agregado no campo de texto e clique em **Apply Filter**.
4. Classifique a lista resultante de LUNs afetados por **IOPS** para visualizar os LUNs que não estão ativos.

Depois de identificar os volumes e LUNs não utilizados, você pode usar o Gerenciador de sistema do ONTAP ou os comandos ONTAP para excluir esses objetos.

## Adicione discos e execute a reconstrução de layout agregado

Você pode adicionar discos a um agregado para aumentar a capacidade de storage e o desempenho desse agregado. Depois de adicionar os discos, você só verá uma melhoria no desempenho após a reconstrução do agregado.

Quando você recebe um evento de limite definido pelo sistema na página de detalhes do evento, o texto de descrição do evento lista o nome do agregado que está tendo o problema. Você pode adicionar discos e reconstruir dados nesse agregado.

Os discos adicionados ao agregado já devem existir no cluster. Se o cluster não tiver discos extras disponíveis, talvez seja necessário entrar em Contato com o administrador ou comprar mais discos. Você pode usar o Gerenciador de sistema do ONTAP ou os comandos ONTAP para adicionar discos a um agregado.

["Relatório técnico 3838: Guia de configuração do subsistema de armazenamento"](#)

## Configurando uma conexão entre um servidor do Unified Manager e um provedor de dados externo

Uma conexão entre um servidor do Unified Manager e um provedor de dados externo permite que você envie dados de desempenho de cluster para um servidor externo para que os gerentes de armazenamento possam traçar as métricas de desempenho usando software de terceiros.

Uma conexão entre um servidor do Unified Manager e um provedor de dados externo é estabelecida por meio da opção de menu chamada "Provedor de dados Externo" no console de manutenção.

### Dados de desempenho que podem ser enviados para um servidor externo

O Unified Manager coleta uma variedade de dados de performance de todos os clusters que ele está monitorando. Você pode enviar grupos específicos de dados para um servidor externo.

Dependendo dos dados de desempenho que você deseja mapear, você pode optar por enviar um dos seguintes grupos de estatísticas:

Grupo de estatísticas	Dados incluídos	Detalhes
Monitor de desempenho	<p>Estatísticas de desempenho de alto nível para os seguintes objetos:</p> <ul style="list-style-type: none"><li>• LUNs</li><li>• Volumes</li></ul>	<p>Esse grupo fornece IOPS total ou latência para todos os LUNs e volumes em todos os clusters monitorados.</p> <p>Este grupo fornece o menor número de estatísticas.</p>

Grupo de estatísticas	Dados incluídos	Detalhes
Utilização de recursos	Estatísticas de utilização de recursos para os seguintes objetos: <ul style="list-style-type: none"> <li>• Nós</li> <li>• Agregados</li> </ul>	Esse grupo fornece estatísticas de utilização do nó e agrega recursos físicos em todos os clusters monitorados.  Ele também fornece as estatísticas coletadas no grupo Monitor de desempenho.
Perfure	Estatísticas de leitura/gravação e por protocolo de baixo nível para todos os objetos rastreados: <ul style="list-style-type: none"> <li>• Nós</li> <li>• Agregados</li> <li>• LUNs</li> <li>• Volumes</li> <li>• Discos</li> <li>• LIFs</li> <li>• Portas/NICs</li> </ul>	Esse grupo fornece quebras de leitura/gravação e por protocolo para todos os sete tipos de objetos rastreados em todos os clusters monitorados.  Ele também fornece as estatísticas coletadas no grupo Monitor de desempenho e no grupo utilização de recursos.  Este grupo fornece o maior número de estatísticas.



Se o nome de um cluster, ou objeto de cluster, for alterado no sistema de armazenamento, ambos os objetos antigos e novos conterão dados de desempenho no servidor externo (chamado de "caminho\_métrico"). Os dois objetos não estão correlacionados com o mesmo objeto. Por exemplo, se você alterar o nome de um volume de ""volume1\_acct"" para ""acct\_vol1"", você verá dados de desempenho antigos para o volume antigo e novos dados de desempenho para o novo volume.

Consulte o artigo 30096 da base de dados de Conhecimento para obter a lista de todos os contadores de desempenho que podem ser enviados para um fornecedor de dados externo.

["Contadores de desempenho do Unified Manager que podem ser exportados para um Fornecedor de dados Externo"](#)

## Configurando o Graphite para receber dados de desempenho do Unified Manager

Graphite é uma ferramenta de software aberto para coletar e grafar dados de desempenho de sistemas de computador. Seu servidor e software Graphite devem ser configurados corretamente para receber dados estatísticos do Unified Manager.

O NetApp não testa ou verifica versões específicas do Graphite ou de outras ferramentas de terceiros.



O servidor Graphite não recebe dados de desempenho para volumes do Unified Manager.

Depois de instalar o Graphite de acordo com as instruções de instalação, você precisa fazer as seguintes alterações para suportar a transferência de dados estatísticos do Unified Manager:

- No `/opt/graphite/conf/carbon.conf` arquivo, o número máximo de arquivos que podem ser criados no servidor Graphite por minuto deve ser definido como `200` (**MAX\_CREATES\_PER\_MINUTE = 200**).

Dependendo do número de clusters em sua configuração e dos objetos de estatísticas que você selecionou para enviar, pode haver milhares de novos arquivos que precisam ser criados inicialmente. Em 200 arquivos por minuto, pode levar 15 minutos ou mais antes que todos os arquivos de métrica sejam criados inicialmente. Depois de todos os arquivos de métrica exclusivos terem sido criados, esse parâmetro não é mais relevante.

- Se você estiver executando o Graphite em um servidor implantado usando um endereço IPv6, o valor para `LINE_RECEIVER_INTERFACE` no `/opt/graphite/conf/carbon.conf` arquivo deve ser alterado de `"0.0.0.0"` para `("LINE_RECEIVER_INTERFACE = :::")`
- `/opt/graphite/conf/storage-schemas.conf` No arquivo, o `retentions` parâmetro deve ser usado para definir a frequência para 5 minutos e o período de retenção para o número de dias relevantes para o seu ambiente.

O período de retenção pode ser o tempo que o seu ambiente permite, mas o valor de frequência deve ser definido para 5 minutos para pelo menos uma configuração de retenção. No exemplo a seguir, uma seção é definida para o Unified Manager usando o `pattern` parâmetro e os valores definem a frequência inicial para 5 minutos e o período de retenção para 100 dias: **[OPM]**

```
pattern = ^netapp-performance\..
```

```
retentions = 5m:100d
```



Se a tag de fornecedor padrão for alterada de `"NetApp-performance"` para algo diferente, essa alteração também deve ser refletida no `pattern` parâmetro.



Se o servidor Graphite não estiver disponível quando o servidor Unified Manager estiver tentando enviar dados de desempenho, os dados não serão enviados e haverá uma lacuna nos dados coletados.

## Configurando uma conexão de um servidor do Unified Manager para um provedor de dados externo

O Unified Manager pode enviar dados de desempenho do cluster para um servidor externo. Você pode especificar o tipo de dados estatísticos que são enviados e o intervalo no qual os dados são enviados.

### Antes de começar

- Você deve ter uma ID de usuário autorizada para fazer login no console de manutenção do servidor do Unified Manager.
- Você deve ter as seguintes informações sobre o provedor de dados externo:
  - Nome do servidor ou endereço IP (IPv4 ou IPv6)
  - Porta padrão do servidor (se não estiver usando a porta padrão 2003)
- Você deve ter configurado o servidor remoto e o software de terceiros para que ele possa receber dados estatísticos do servidor do Unified Manager.



- Você deve saber qual grupo de estatísticas deseja enviar:
  - PERFORMANCE\_INDICATOR: Estatísticas do monitor de desempenho
  - RESOURCE\_USAGE: Estatísticas de utilização de recursos e de monitoramento de desempenho
  - DRILL\_down: Todas as estatísticas
- Você deve saber o intervalo de tempo no qual deseja transmitir estatísticas: 5, 10 ou 15 minutos

Por padrão, o Unified Manager coleta estatísticas em intervalos de 5 minutos. Se definir o intervalo de transmissão para 10 (ou 15) minutos, a quantidade de dados que é enviada durante cada transmissão é duas (ou três) vezes maior do que quando se utiliza o intervalo predefinido de 5 minutos.



Se você alterar o intervalo de coleta de desempenho do Unified Manager para 10 ou 15 minutos, altere o intervalo de transmissão para que ele seja igual ou maior que o intervalo de coleta do Unified Manager.

Você pode configurar uma conexão entre um servidor do Unified Manager e um servidor de provedor de dados externo.

### Passos

1. Faça login como usuário de manutenção no console de manutenção do servidor do Unified Manager.

Os prompts do console de manutenção do Unified Manager são exibidos.

2. No console de manutenção, digite o número da opção de menu **External Data Provider**.

É apresentado o menu External Server Connection (ligação ao servidor externo).

3. Digite o número da opção de menu **Add/Modify Server Connection**.

As informações de conexão do servidor atual são exibidas.

4. Quando solicitado, digite **y** para continuar.

5. Quando solicitado, insira o endereço IP ou o nome do servidor de destino e as informações da porta do servidor (se diferente da porta padrão 2003).

6. Quando solicitado, digite **y** para verificar se as informações inseridas estão corretas.

7. Pressione qualquer tecla para retornar ao menu conexão do servidor externo.

8. Digite o número da opção de menu **Modificar configuração do servidor**.

As informações de configuração do servidor atual são exibidas.

9. Quando solicitado, digite **y** para continuar.

10. Quando solicitado, insira o tipo de estatísticas a enviar, o intervalo de tempo no qual as estatísticas são enviadas e se você deseja ativar a transmissão de estatísticas agora:

Para..	Digite...
ID do grupo de estatísticas	<p><b>0</b> - PERFORMANCE_INDICATOR (padrão)</p> <p><b>1</b> - RECURSO_UTILIZAÇÃO</p> <p><b>2</b> - DRILL_DOWN</p>
Etiqueta do fornecedor	<p>Um nome descritivo para a pasta onde as estatísticas serão armazenadas no servidor externo. "NetApp-performance" é o nome padrão, mas você pode inserir outro valor.</p> <p>Usando notação pontilhada, você pode definir uma estrutura de pastas hierárquica. Por exemplo, ao inserir <b>stats.performance.netapp</b> as estatísticas estará localizado em <b>stats &gt; performance &gt; NetApp</b>.</p>
Intervalo de transmissão	<b>5</b> (predefinição), <b>10</b> , ou <b>15</b> minutos
Ativar/desativar	<p><b>0</b> - Desativar</p> <p><b>1</b> - Ativar (predefinição)</p>

11. Quando solicitado, digite **y** para verificar se as informações inseridas estão corretas.
12. Pressione qualquer tecla para retornar ao menu conexão do servidor externo.
13. Digite **x** para sair do console de manutenção.

Depois de configurar a ligação, os dados de desempenho selecionados são enviados para o servidor de destino no intervalo de tempo especificado. Leva alguns minutos antes que as métricas comecem a aparecer na ferramenta externa. Talvez seja necessário atualizar o navegador para ver as novas métricas na hierarquia de métricas.

# Monitorar e gerenciar a integridade do cluster

## Introdução ao monitoramento da saúde do Active IQ Unified Manager

O Active IQ Unified Manager (antigo Gerenciador Unificado de OnCommand) ajuda você a monitorar um grande número de sistemas que executam o software ONTAP por meio de uma interface de usuário centralizada. A infraestrutura de servidor do Unified Manager oferece escalabilidade, capacidade de suporte e recursos aprimorados de monitoramento e notificação.

Os principais recursos do Unified Manager incluem monitoramento, alerta, gerenciamento de disponibilidade e capacidade dos clusters, gerenciamento de recursos de proteção e agrupamento de dados de diagnóstico e envio para o suporte técnico.

Você pode usar o Unified Manager para monitorar os clusters. Quando ocorrem problemas no cluster, o Unified Manager notifica você sobre os detalhes de tais problemas por meio de eventos. Alguns eventos também fornecem uma ação corretiva que você pode tomar para corrigir os problemas. Você pode configurar alertas para eventos para que, quando os problemas ocorrem, você seja notificado por e-mail e traps SNMP.

Você pode usar o Unified Manager para gerenciar objetos de storage em seu ambiente associando-os a anotações. Você pode criar anotações personalizadas e associar dinamicamente clusters, máquinas virtuais de armazenamento (SVMs) e volumes às anotações por meio de regras.

Você também pode Planejar os requisitos de armazenamento dos objetos de cluster usando as informações fornecidas nos gráficos de capacidade e integridade para o respectivo objeto de cluster.

### Capacidade física e lógica

O Unified Manager faz uso dos conceitos de espaço físico e lógico usados para objetos de storage do ONTAP.

- Capacidade física: O espaço físico refere-se aos blocos físicos de armazenamento utilizados no volume. "Capacidade física usada" geralmente é menor que a capacidade lógica usada devido à redução de dados de recursos de eficiência de storage (como deduplicação e compactação).
- Capacidade lógica: O espaço lógico refere-se ao espaço utilizável (os blocos lógicos) em um volume. O espaço lógico refere-se a como o espaço teórico pode ser usado, sem levar em conta os resultados da deduplicação ou compressão. "Espaço lógico usado" é o espaço físico usado, além da economia com recursos de eficiência de storage (como deduplicação e compactação) que foram configurados. Essa medida geralmente parece maior do que a capacidade física usada, pois isso não reflete a compressão de dados e outras reduções no espaço físico. Assim, a capacidade lógica total poderia ser maior do que o espaço provisionado.

### Unidades de medição da capacidade

O Unified Manager calcula a capacidade de armazenamento com base em unidades binárias de 1024 (2,10) bytes. No ONTAP 9.10,0 e anterior, essas unidades foram exibidas como KB, MB, GB, TB e PB. A partir do ONTAP 9.10,1, eles são exibidos no Gerenciador Unificado como KiB, MiB, GiB, TiB e PiB.



As unidades usadas para a taxa de transferência continuam a ser kilobytes por segundo (Kbps), megabytes por segundo (Mbps), Gigabytes por segundo (Gbps) ou Terabytes por segundo (Tbps) e assim por diante, para todas as versões do ONTAP.

Unidade de capacidade exibida no Gerenciador Unificado para ONTAP 9.10,0 e anterior	Unidade de capacidade exibida no Gerenciador Unificado para o ONTAP 9.10,1	Cálculo	Valor em bytes
KB	KiB	1024	1024 bytes
MB	MiB	1024 * 1024	1.048.576 bytes
GB	GiB	1024 * 1024 * 1024	1.073.741.824 bytes
TB	TiB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 bytes

## Recursos de monitoramento de integridade do Unified Manager

O Unified Manager foi desenvolvido em uma infraestrutura de servidor que oferece escalabilidade, capacidade de suporte e recursos aprimorados de monitoramento e notificação. O Unified Manager é compatível com o monitoramento de sistemas que executam o software ONTAP.

O Unified Manager inclui os seguintes recursos:

- Detecção, monitoramento e notificações de sistemas instalados com o software ONTAP:
  - Objetos físicos: Nós, discos, compartimentos de disco, pares SFO, portas e Flash Cache
  - Objetos lógicos: Clusters, máquinas virtuais de storage (SVMs), agregados, volumes, LUNs, namespaces, qtrees, LIFs, cópias Snapshot, caminhos de junção, compartilhamentos NFS, compartilhamentos SMB, cotas de usuários e grupos, grupos de políticas de QoS e grupos de iniciadores
  - Protocolos: CIFS, NFS, FC, iSCSI, NVMe e FCoE
  - Eficiência de storage: Agregados SSD, agregados de Flash Pool, agregados FabricPool, deduplicação e compactação
  - Proteção: Relacionamentos SnapMirror (síncronos e assíncronos) e relacionamentos SnapVault
- Visualização do estado de detecção e monitorização do cluster
- Configurações MetroCluster em FC e IP: Visualização e monitoramento da configuração, problemas e status de conectividade dos componentes do cluster. Switches e bridges MetroCluster para configurações MetroCluster em FC
- Infraestrutura de alertas, eventos e limites aprimorados
- LDAP, LDAPS, autenticação SAML e suporte ao usuário local
- RBAC (para um conjunto predefinido de funções)
- AutoSupport e pacote de suporte

- Painel aprimorado para mostrar a capacidade, disponibilidade, proteção e integridade de performance do ambiente
- Interoperabilidade de movimentação de volume, histórico de movimentação de volume e histórico de mudança de caminho de junção
- Área de escopo de impactos que exibe graficamente os recursos que são afetados para eventos como alguns discos com falha, espelhamento agregado MetroCluster degradado e discos de reserva MetroCluster deixados para trás eventos
- Possível área de efeito que exibe o efeito dos eventos MetroCluster
- Área de ações corretivas sugeridas que exibe as ações que podem ser executadas para resolver eventos como alguns discos com falha, espelhamento agregado MetroCluster degradado e discos sobressalentes MetroCluster deixados para trás eventos
- Recursos que podem ser afetados área que exibe os recursos que podem ser afetados para eventos como o evento volume Offline, o evento volume restrito e o evento espaço em volume provisionado por thin
- Suporte a SVMs com FlexVol ou FlexGroup volumes
- Suporte para monitoramento de volumes de raiz de nós
- Monitoramento aprimorado de cópia Snapshot, incluindo computação de espaço que pode ser recuperado e exclusão de cópias Snapshot
- Anotações para objetos de armazenamento
- Relatar a criação e o gerenciamento de informações de objetos de storage, como capacidade física e lógica, utilização, economia de espaço, desempenho e eventos relacionados
- Integração com o OnCommand Workflow Automation para executar fluxos de trabalho

O repositório de automação do storage contém pacotes de fluxo de trabalho de storage automatizado certificados pela NetApp, desenvolvidos para uso com o OnCommand Workflow Automation (WFA). Você pode baixar os pacotes e depois importá-los para O WFA para executá-los. Os fluxos de trabalho automatizados estão disponíveis aqui:

["Armazenamento de automação de storage"](#)

## **Interfaces do Unified Manager usadas para gerenciar a integridade do sistema de storage**

Essas seções contêm informações sobre as duas interfaces de usuário fornecidas pelo Active IQ Unified Manager para solucionar problemas de capacidade, disponibilidade e proteção de storage de dados. As duas UIs são a IU da Web do Unified Manager e o console de manutenção.

Se você quiser usar os recursos de proteção no Unified Manager, também deverá instalar e configurar o OnCommand Workflow Automation (WFA).

### **IU da Web do Unified Manager**

A IU da Web do Unified Manager permite que um administrador monitore e solucione problemas de cluster relacionados à capacidade, disponibilidade e proteção de storage de dados.

Essas seções descrevem alguns fluxos de trabalho comuns que um administrador pode seguir para solucionar problemas de capacidade de storage, disponibilidade de dados ou proteção exibidos na IU da Web do Unified

Manager.

### **Consola de manutenção**

O console de manutenção do Unified Manager permite que um administrador monitore, diagnostique e solucione problemas do sistema operacional, problemas de atualização de versão, problemas de acesso do usuário e problemas de rede relacionados ao próprio servidor do Unified Manager. Se a IU da Web do Unified Manager não estiver disponível, o console de manutenção será a única forma de acesso ao Unified Manager.

Você pode usar essas informações para acessar o console de manutenção e usá-lo para resolver problemas relacionados ao funcionamento do servidor do Unified Manager.

## **Gerenciamento e monitoramento de clusters e integridade de objetos do cluster**

O Unified Manager usa consultas periódicas de API e um mecanismo de coleta de dados para coletar dados dos clusters. Ao adicionar clusters ao banco de dados do Unified Manager, você pode monitorar e gerenciar esses clusters para verificar se há riscos de disponibilidade e capacidade.

### **Compreender o monitoramento do cluster**

É possível adicionar clusters ao banco de dados do Unified Manager para monitorar os clusters quanto à disponibilidade, capacidade e outros detalhes, como uso da CPU, estatísticas de interface, espaço livre em disco, uso de qtree e ambiente de chassi.

Os eventos são gerados se o status for anormal ou quando um limite predefinido for violado. Se configurado para isso, o Unified Manager envia uma notificação para um destinatário especificado quando um evento aciona um alerta.

### **Compreendendo os volumes raiz dos nós**

Você pode monitorar o volume raiz do nó usando o Unified Manager. A prática recomendada é que o volume raiz do nó deve ter capacidade suficiente para impedir que o nó caia.

Quando a capacidade usada do volume raiz do nó excede 80% da capacidade total do volume raiz do nó, o evento espaço quase cheio do volume raiz do nó é gerado. Você pode configurar um alerta para o evento para receber uma notificação. Você pode tomar as medidas apropriadas para impedir que o nó fique inativo usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.



A funcionalidade de monitoramento de volumes de raiz de nós não está disponível se os clusters executarem a versão ONTAP 9.14,1 ou posterior.

### **Compreensão de eventos e limites para agregados de raiz de nós**

Você pode monitorar o agregado de raiz de nó usando o Unified Manager. A prática recomendada é provisionar rapidamente o volume raiz no agregado raiz para evitar que o nó pare.

Por padrão, eventos de capacidade e performance não são gerados para agregados de raiz. Além disso, os valores de limite usados pelo Unified Manager não são aplicáveis aos agregados de raiz de nós. Somente um representante de suporte técnico pode modificar as configurações para que esses eventos sejam gerados. Quando as configurações são modificadas pelo representante do suporte técnico, os valores limite de capacidade são aplicados ao agregado raiz do nó.

Você pode tomar as medidas apropriadas para impedir que o nó pare usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.



A funcionalidade de monitorar agregados de raiz de nós não estará disponível se os clusters executarem a versão ONTAP 9.14,1 ou posterior.

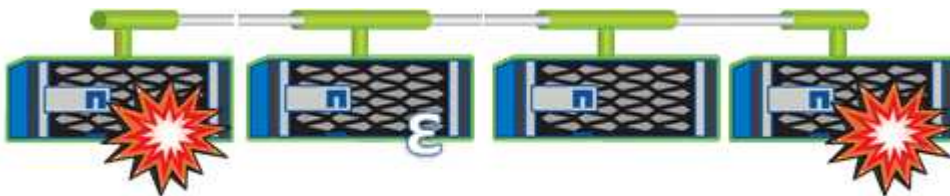
## Compreensão do quórum e do epsilon

O quórum e o epsilon são medidas importantes de integridade e função do cluster que, em conjunto, indicam como os clusters abordam potenciais desafios de comunicação e conectividade.

*Quorum* é uma pré-condição para um cluster totalmente funcional. Quando um cluster está no quórum, uma maioria simples dos nós é saudável e pode se comunicar uns com os outros. Quando o quorum é perdido, o cluster perde a capacidade de realizar operações normais de cluster. Apenas uma coleção de nós pode ter quórum de cada vez, porque todos os nós compartilham coletivamente uma única visualização dos dados. Portanto, se dois nós não-comunicantes forem permitidos modificar os dados de maneiras divergentes, não será mais possível reconciliar os dados em uma única visualização de dados.

Cada nó no cluster participa de um protocolo de votação que elege um nó mestre; cada nó restante é um secundário. O nó principal é responsável pela sincronização de informações no cluster. Quando o quórum é formado, ele é mantido por votação contínua. Se o nó mestre ficar offline e o cluster ainda estiver no quórum, um novo mestre será eleito pelos nós que permanecem online.

Como existe a possibilidade de um empate em um cluster que tem um número par de nós, um nó tem um peso de votação fracionário extra chamado epsilon. Se a conectividade entre duas partes iguais de um cluster grande falhar, o grupo de nós que contém epsilon mantém quórum, assumindo que todos os nós estão saudáveis. Por exemplo, a ilustração a seguir mostra um cluster de quatro nós no qual dois dos nós falharam. No entanto, como um dos nós sobreviventes possui epsilon, o cluster permanece no quórum, embora não haja uma maioria simples de nós saudáveis.



O Epsilon é atribuído automaticamente ao primeiro nó quando o cluster é criado. Se o nó que mantém o epsilon não estiver saudável, assumir o seu parceiro de alta disponibilidade ou for assumido pelo parceiro de alta disponibilidade, o epsilon será reatribuído automaticamente a um nó saudável em um par de HA diferente.

Colocar um nó off-line pode afetar a capacidade do cluster de permanecer no quorum. Portanto, o ONTAP emite uma mensagem de aviso se você tentar uma operação que irá tirar o cluster do quórum ou então colocar uma interrupção longe de uma perda de quórum. Você pode desativar as mensagens de aviso de quórum usando o comando de modificação de opções de quórum de cluster no nível de privilégio avançado.

Em geral, assumindo uma conectividade confiável entre os nós do cluster, um cluster maior é mais estável do que um cluster menor. O requisito de quórum de uma maioria simples de metade dos nós mais o epsilon é mais fácil de manter em um cluster de 24 nós do que em um cluster de dois nós.

Um cluster de dois nós apresenta alguns desafios únicos para manter o quórum. Os clusters de dois nós usam o cluster HA, no qual nenhum nó detém o epsilon; em vez disso, ambos os nós são continuamente polidos para garantir que, se um nó falhar, o outro terá acesso completo de leitura e gravação aos dados, bem como acesso a interfaces lógicas e funções de gerenciamento.

## Visualizar a lista de cluster e os detalhes

Você pode usar a visualização integridade: Todos os clusters para visualizar o inventário de clusters. A visualização capacidade: Todos os clusters permite visualizar informações resumidas sobre capacidade de storage e utilização em todos os clusters.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Você também pode exibir detalhes de clusters individuais, como a integridade do cluster, capacidade, configuração, LIFs, nós e discos nesse cluster usando a página de detalhes de cluster / integridade.

Os detalhes na exibição integridade: Todos os clusters, capacidade: Todos os clusters e a página de detalhes de cluster / integridade ajudam a Planejar seu storage. Por exemplo, antes de provisionar um novo agregado, você pode selecionar um cluster específico na exibição integridade: Todos os clusters e obter detalhes de capacidade para determinar se o cluster tem o espaço necessário.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > clusters**.
2. No menu Exibir, selecione a exibição **Saúde: Todos os clusters** para exibir informações de integridade ou **capacidade: Todos os clusters** para exibir detalhes sobre capacidade de armazenamento e utilização em todos os clusters.
3. Clique no nome de um cluster para ver os detalhes completos do cluster na página de detalhes **Cluster / Health**.

### Informações relacionadas

- ["Página de detalhes de cluster / Saúde"](#)
- ["Desempenho: Visualização de todos os clusters"](#)
- ["Monitoramento de configurações do MetroCluster"](#)
- ["Visualização do status de segurança dos clusters e das VMs de storage"](#)
- ["Quais critérios de segurança estão sendo avaliados"](#)

## Verificação da integridade dos clusters em uma configuração do MetroCluster

Você pode usar o Active IQ Unified Manager (Unified Manager) para verificar a integridade operacional dos clusters e seus componentes, nas configurações MetroCluster em FC e MetroCluster em IP. Se os clusters estiverem envolvidos em um evento de desempenho detetado pelo Unified Manager, o status de integridade pode ajudá-lo a determinar se um problema de hardware ou software contribuiu para o evento.



## Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter analisado um evento de desempenho para uma configuração do MetroCluster e obtido o nome do cluster envolvido.
- Ambos os clusters na configuração do MetroCluster por FC e IP precisam ser monitorados pela mesma instância do Unified Manager.

## Determinando a integridade do cluster na configuração de MetroCluster em FC

Siga estas etapas para determinar a integridade do cluster em uma configuração MetroCluster sobre FC.

### Passos

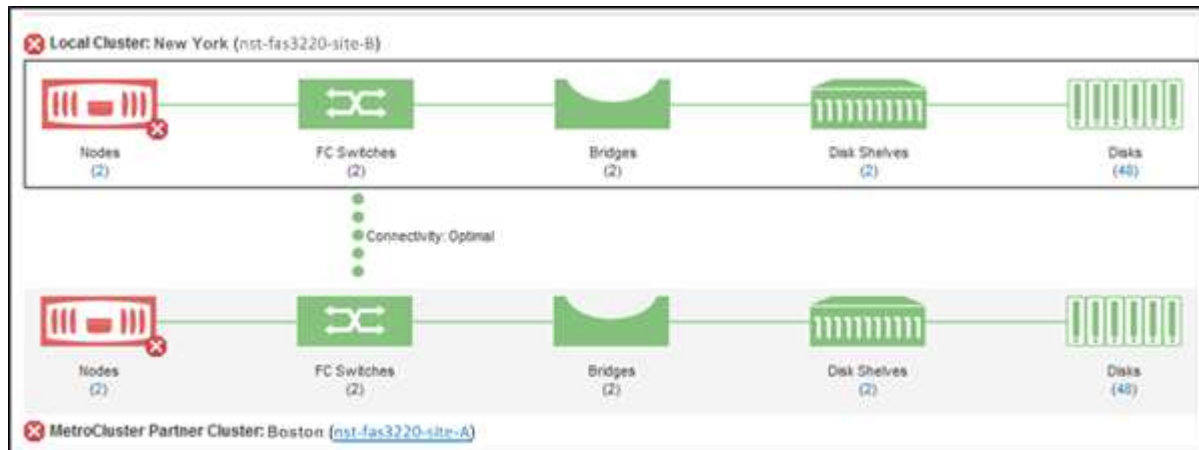
1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos** para exibir a lista de eventos.
2. No painel de filtro, selecione todos os filtros MetroCluster na categoria **tipo de fonte**. Você vê todos os eventos criados no seu ambiente para todas as configurações do MetroCluster.
3. Ao lado de um evento do MetroCluster, clique no nome do cluster.



Se não forem apresentados eventos MetroCluster, pode utilizar a barra de pesquisa para procurar o nome do cluster envolvido no evento relacionado com a configuração MetroCluster sobre FC.

A exibição Saúde: Todos os clusters é exibida com informações detalhadas sobre o evento.

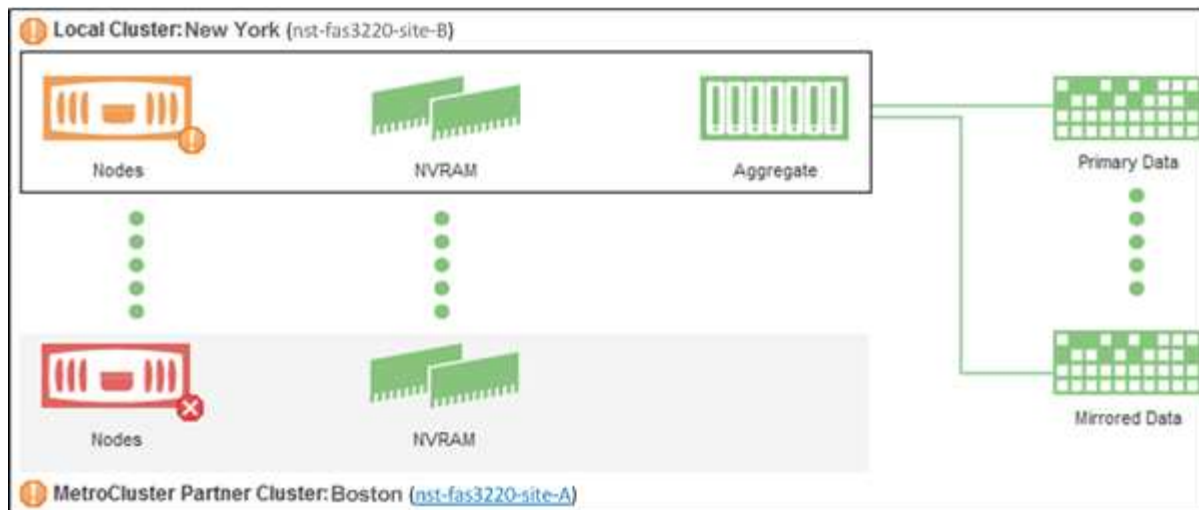
4. Selecione a guia **conetividade MetroCluster** para exibir a integridade da conexão entre o cluster selecionado e seu cluster de parceiros.



Neste exemplo, são apresentados os nomes e os componentes do cluster local e do respectivo cluster de parceiros. Um ícone amarelo ou vermelho indica um evento de saúde para o componente realçado. O ícone conetividade representa o link entre os clusters. Você pode apontar o cursor do Mouse para um ícone para exibir informações de eventos ou clicar no ícone para exibir os eventos. Um problema de integridade em qualquer cluster pode ter contribuído para o evento de desempenho.

O Unified Manager monitora o componente NVRAM do link entre os clusters. Se o ícone de switches FC no cluster local ou de parceiros ou o ícone de conetividade estiver vermelho, um problema de integridade do link pode ter causado o evento de desempenho.

5. Selecione a guia **replicação MetroCluster**.



Neste exemplo, se o ícone NVRAM no cluster local ou de parceiros estiver amarelo ou vermelho, um problema de integridade com o NVRAM pode ter causado o evento de desempenho. Se não houver ícones vermelhos ou amarelos na página, um problema de desempenho no cluster de parceiros pode ter causado o evento de desempenho.

### Determinando a integridade do cluster na configuração MetroCluster sobre IP

Siga estas etapas para determinar a integridade do cluster em uma configuração MetroCluster sobre IP.

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos** para exibir a lista de eventos.
2. No painel de filtro, na categoria **tipo de fonte**, selecione o `MetroCluster Relationship` filtro. Você vê todos os eventos criados no seu ambiente para todas as configurações do MetroCluster.



Se não conseguir ver os eventos MetroCluster reportados, pode utilizar a barra de pesquisa para pesquisar pelo nome do cluster envolvido no evento relacionado com a configuração MetroCluster sobre IP.

3. Ao lado do evento MetroCluster relevante, clique no nome do cluster. A página clusters é exibida com os detalhes desse cluster. Para obter informações sobre como determinar problemas de saúde, "[Monitore problemas de conectividade na configuração MetroCluster sobre IP](#)" consulte .

### Visualização do status de integridade e capacidade de todos os clusters do SAN Array

Você pode usar as páginas de inventário de cluster para exibir o status de integridade e capacidade dos clusters de todos os Arrays SAN.

#### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Você pode exibir informações gerais de todos os clusters de storage SAN na exibição integridade: Todos os clusters e capacidade: Todos os clusters. Além disso, você pode exibir detalhes na página de detalhes do Cluster / Health.

#### Passos

1. No painel de navegação esquerdo, clique em **Storage > clusters**.
2. Certifique-se de que a coluna "personalidade" seja exibida na visualização **Saúde: Todos os clusters** ou adicione-a usando o controle **Mostrar / Ocultar**.

Essa coluna exibe "All SAN Array" para os clusters All SAN Array.

3. Reveja as informações.
4. Para exibir informações sobre a capacidade de storage nesses clusters, selecione a visualização capacidade: Todos os clusters.
5. Para exibir informações detalhadas sobre integridade e capacidade de storage nesses clusters, clique no nome de um cluster All SAN Array.

Exiba os detalhes nas guias integridade, capacidade e nós na página Detalhes do cluster/integridade

## Exibindo a lista de nós e os detalhes

Você pode usar a visualização integridade: Todos os nós para exibir a lista de nós nos clusters. Você pode usar a página de detalhes de Cluster / Health para exibir informações detalhadas sobre nós que fazem parte do cluster monitorado.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Você pode visualizar detalhes como o estado do nó, o cluster que contém o nó, os detalhes de capacidade agregada (usada e total) e os detalhes de capacidade bruta (utilizável, sobressalente e total). Você também pode obter informações sobre pares de HA, compartimentos de discos e portas.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > Nodes**.
2. Na exibição **Saúde: Todos os nós**, clique no nó cujos detalhes você deseja exibir.

As informações detalhadas para o nó selecionado são apresentadas na página Cluster / Health details (Detalhes do Cluster/Health). O painel esquerdo exibe a lista de pares de HA. Por padrão, os Detalhes da HA estão abertos, que exibe detalhes do estado da HA e eventos relacionados ao par de HA selecionado.

3. Para exibir outros detalhes sobre o nó, execute a ação apropriada:

Para ver...	Clique em...
Detalhes sobre as gavetas de disco	<b>Prateleiras de disco.</b>
Informações relacionadas com a porta	<b>Portos.</b>

Para obter mais informações, consulte:

- ["Performance: Visualização de todos os nós"](#)
- ["Exibindo o nó e agregar valores de IOPS disponíveis"](#)
- ["Exibindo valores de capacidade de desempenho agregado e nó usados"](#)

## Gerando um relatório de inventário de hardware para renovação de contrato

Você pode gerar um relatório que contém uma lista completa de informações de cluster e nó, como números de modelo de hardware e números de série, tipos e contagens de disco, licenças instaladas e muito mais. Este relatório é útil para a renovação de contratos em sites seguros ("dark" sites) que não estão conectados à plataforma NetAppactive IQ.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > Nodes**.
2. Vá para a visualização **Saúde: Todos os nós** ou **desempenho: Todos os nós**.
3. Selecione **relatórios > \* > Relatório de inventário de hardware\***.

O relatório de inventário de hardware é baixado como um arquivo .csv com informações completas a partir da data atual.

4. Forneça essas informações ao seu Contato de suporte da NetApp para renovação de contrato.

## Exibindo a lista e os detalhes da VM de armazenamento

Na visualização integridade: Todas as VMs de armazenamento, você pode monitorar seu inventário de máquinas virtuais de armazenamento (SVMs). Você pode usar a página Storage VM / Health details para exibir informações detalhadas sobre SVMs que são monitoradas.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

É possível visualizar os detalhes do SVM, como capacidade, eficiência e configuração de um SVM. Você também pode exibir informações sobre os dispositivos relacionados e alertas relacionados para esse SVM.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > Storage VMs**.
2. Escolha uma das seguintes maneiras de exibir os detalhes do SVM:
  - Para exibir informações sobre a integridade de todos os SVMs em todos os clusters, no menu Exibir, selecione integridade: Exibição de todas as VMs de armazenamento.
  - Para exibir os detalhes completos, clique no nome da VM de armazenamento.

Você também pode visualizar os detalhes completos clicando em **Exibir detalhes** na caixa de diálogo Detalhes mínimos.

3. Visualize os objetos relacionados ao SVM clicando em **Exibir relacionado** na caixa de diálogo Detalhes mínimos.

### Informações relacionadas

- ["VM de storage: Página de detalhes de integridade"](#)
- ["Performance: Visualização de todas as VMs de storage"](#)
- ["Segurança: Vista anti-ransomware"](#)
- ["Visualização do status de segurança dos clusters e das VMs de storage"](#)
- ["Relacionamento: Todos os relacionamentos são exibidos"](#)

## Exibindo a lista de agregados e os detalhes

Na visualização Saúde: Todos os agregados, você pode monitorar seu inventário de agregados. A visualização capacidade: Todos os agregados permite visualizar informações sobre a capacidade e a utilização de agregados em todos os clusters.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Você pode exibir detalhes como capacidade e configuração de agregados e informações de disco na página de detalhes de agregado / integridade. Você pode usar esses detalhes antes de configurar as configurações de limite, se necessário.

### Passos

1. No painel de navegação à esquerda, clique em **Storage > Aggregates**.
2. Escolha uma das seguintes maneiras de exibir os detalhes agregados:
  - Para exibir informações sobre a integridade de todos os agregados em todos os clusters, no menu Exibir, selecione integridade: Exibição todos os agregados.
  - Para exibir informações sobre a capacidade e a utilização de todos os agregados em todos os clusters, no menu Exibir, selecione capacidade: Todos os agregados.
  - Para ver os detalhes completos, clique no nome do agregado.

Você também pode visualizar os detalhes completos clicando em **Exibir detalhes** na caixa de diálogo Detalhes mínimos.

3. Visualize os objetos relacionados ao agregado clicando em **Exibir relacionado** na caixa de diálogo Detalhes mínimos.

### Informações relacionadas

- ["Página de detalhes agregados / Saúde"](#)
- ["Performance: Visualização de todos os agregados"](#)
- ["Personalização de relatórios de capacidade agregada"](#)

## Visualização de informações de capacidade do FabricPool

É possível visualizar as informações de capacidade do FabricPool para clusters, agregados e volumes no inventário de capacidade e performance, bem como nas páginas de detalhes desses objetos. Essas páginas também exibem informações de espelho do FabricPool quando um nível de espelho foi configurado.

Essas páginas exibem informações como a capacidade disponível na camada de performance local e na

camada de nuvem, quanta capacidade está sendo usada em ambas as camadas, quais agregados estão anexados a uma camada de nuvem e quais volumes estão implementando os recursos do FabricPool movendo certas informações para a camada de nuvem.

Quando um nível de nuvem é espelhado para outro provedor de nuvem (o "nível de erro"), ambos os níveis de nuvem são exibidos na página de detalhes de agregado / Saúde.

### Passos

1. Execute um dos seguintes procedimentos:

Para exibir informações de capacidade para...	Faça isso...
Clusters	<ol style="list-style-type: none"><li>a. Na exibição capacidade: Todos os clusters, clique em um cluster.</li><li>b. Na página Detalhes do Cluster / Health, clique na guia <b>Configuration</b>.</li></ol> <p>O visor mostra os nomes de quaisquer camadas de nuvem às quais esse cluster está conectado.</p>
Agregados	<ol style="list-style-type: none"><li>a. Na visualização capacidade: Todos os agregados, clique em um agregado onde o campo tipo indica "'SSD (FabricPool)" ou "'HDD (FabricPool)".</li><li>b. Na página de detalhes de agregado / Saúde, clique na guia <b>capacidade</b>.</li></ol> <p>O visor mostra a capacidade total usada no nível de nuvem.</p> <ol style="list-style-type: none"><li>c. Clique na guia <b>informações do disco</b>.</li></ol> <p>O visor mostra o nome do nível de nuvem e a capacidade utilizada.</p> <ol style="list-style-type: none"><li>d. Clique na guia <b>Configuração</b>.</li></ol> <p>O visor mostra o nome do nível de nuvem e outras informações detalhadas sobre o nível de nuvem.</p>

Para exibir informações de capacidade para...	Faça isso...
Volumes	<p>a. Na exibição capacidade: Todos os volumes, clique em um volume em que um nome de política aparece no campo ""Política de disposição em categorias"".</p> <p>b. Na página de detalhes de volume / Saúde, clique na guia <b>Configuração</b>.</p> <p>O visor mostra o nome da política de disposição em camadas do FabricPool atribuída ao volume.</p>

- Na página **análise de carga de trabalho**, você pode selecionar ""Visão de nível de nuvem"" na área **tendência de capacidade** para ver a capacidade que está sendo usada no nível de desempenho local e no nível de nuvem no mês anterior.

Para obter mais informações sobre agregados FabricPool, "[Visão geral de discos e agregados](#)" consulte .

## Visualização dos detalhes do pool de armazenamento

Você pode visualizar os detalhes do pool de storage para monitorar a integridade do pool de storage, o cache total e disponível e as alocações usadas e disponíveis.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

### Passos

- No painel de navegação à esquerda, clique em **Storage > Aggregates**.
- Clique em um nome de agregado.

Os detalhes do agregado selecionado são exibidos.

- Clique na guia **informações do disco**.

São apresentadas informações detalhadas sobre o disco.



A tabela Cache é exibida somente quando o agregado selecionado estiver usando um pool de armazenamento.

- Na tabela Cache, mova o ponteiro sobre o nome do pool de armazenamento necessário.

Os detalhes do pool de armazenamento são exibidos.

## Visualizar a lista de volumes e os detalhes

Na visualização Saúde: Todos os volumes, você pode monitorar seu inventário de volumes. A visualização capacidade: Todos os volumes permite visualizar informações sobre a capacidade e a utilização de volumes em um cluster.

## Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Você também pode usar a página Detalhes de volume / Saúde para visualizar informações detalhadas sobre volumes monitorados, incluindo a capacidade, eficiência, configuração e proteção dos volumes. Você também pode exibir informações sobre os dispositivos relacionados e alertas relacionados para um volume específico.

## Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. Escolha uma das seguintes formas de visualizar os detalhes do volume:
  - Para exibir informações detalhadas sobre a integridade dos volumes em um cluster, no menu Exibir, selecione Saúde: Exibição todos os volumes.
  - Para exibir informações detalhadas sobre a capacidade e a utilização de volumes em um cluster, no menu Exibir, selecione capacidade: Exibição todos os volumes.
  - Para ver os detalhes completos, clique no nome do volume.

Você também pode visualizar os detalhes completos clicando em **Exibir detalhes** na caixa de diálogo Detalhes mínimos.

3. **Opcional:** Veja os objetos relacionados ao volume clicando em **Exibir relacionado** na caixa de diálogo Detalhes mínimos.

## Informações relacionadas

- ["Volume: Página de detalhes de saúde"](#)
- ["Performance: Visualização de todos os volumes"](#)
- ["Segurança: Vista anti-ransomware"](#)
- ["Exibindo relações de proteção de volume"](#)
- ["Criando um relatório para exibir gráficos de capacidade de volume disponíveis"](#)

## Exibição de detalhes sobre compartilhamentos NFS

É possível visualizar detalhes sobre todos os compartilhamentos NFS, como status, caminho associado ao volume (volumes FlexGroup ou volumes FlexVol), níveis de acesso dos clientes aos compartilhamentos NFS e a política de exportação definida para os volumes exportados. Uso da visualização integridade: Todos os compartilhamentos NFS para ver todos os compartilhamentos NFS em todos os clusters monitorados e usar a página de detalhes de integridade/VM de storage para visualizar todos os compartilhamentos NFS em uma máquina virtual de storage específica (SVM).

## Antes de começar

- A licença NFS deve estar ativada no cluster.
- As interfaces de rede que atendem aos compartilhamentos NFS devem ser configuradas.
- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

## Passo

1. No painel de navegação à esquerda, siga as etapas abaixo, dependendo se você deseja exibir todos os compartilhamentos NFS ou apenas os compartilhamentos NFS de um SVM específico.



Para...	Siga estes passos...
Ver todos os compartilhamentos NFS	Clique em <b>Storage &gt; compartilhamentos NFS</b>
Visualizar compartilhamentos NFS em um único SVM	a. Clique em <b>Storage &gt; Storage VMs</b> b. Clique no SVM para o qual você deseja visualizar os detalhes dos compartilhamentos NFS. c. Na página Storage VM / Health details, clique na guia <b>NFS shares</b> .

Para obter mais informações, "[Provisionar volumes de compartilhamento de arquivos](#)" consulte e "[Provisionamento de compartilhamentos de arquivos CIFS e NFS com o uso de APIs](#)".

## Exibindo detalhes sobre compartilhamentos SMB/CIFS

Você pode exibir detalhes sobre todos os compartilhamentos SMB/CIFS, como nome do compartilhamento, caminho de junção, contendo objetos, configurações de segurança e políticas de exportação definidas para o compartilhamento. Use a visualização integridade: Todos os compartilhamentos SMB para ver todos os compartilhamentos SMB em todos os clusters monitorados e use a página de detalhes de integridade/VM de storage para exibir todos os compartilhamentos SMB em uma máquina virtual de storage específica (SVM).

### Antes de começar

- A licença CIFS deve estar ativada no cluster.
- As interfaces de rede que atendem aos compartilhamentos SMB/CIFS devem ser configuradas.
- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.



Compartilhamentos em pastas não são exibidos.

### Passo

1. No painel de navegação à esquerda, siga as etapas abaixo, dependendo se você deseja exibir todos os compartilhamentos SMB/CIFS ou apenas os compartilhamentos de um SVM específico.

Para...	Siga estes passos...
Ver todos os compartilhamentos SMB/CIFS	Clique em <b>Storage &gt; SMB shares</b>
Veja compartilhamentos de SMB/CIFS em uma única SVM	a. Clique em <b>Storage &gt; Storage VMs</b> b. Clique no SVM para o qual você deseja exibir os detalhes do compartilhamento SMB/CIFS. c. Na página Storage VM / Health details, clique na guia <b>SMB shares</b> .

Para obter mais informações, "[Provisionamento de compartilhamentos de arquivos CIFS e NFS com o uso de APIs](#)" consulte .

## Exibição da lista de cópias Snapshot

É possível exibir a lista de cópias Snapshot de um volume selecionado. Você pode usar a lista de cópias Snapshot para calcular a quantidade de espaço em disco que pode ser recuperado se uma ou mais cópias Snapshot forem excluídas e excluir as cópias Snapshot, se necessário.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- O volume que contém as cópias Snapshot precisa estar online.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. Na exibição **Saúde: Todos os volumes**, selecione o volume que contém as cópias Snapshot que deseja exibir.
3. Na página de detalhes **volume / Saúde**, clique na guia **capacidade**.
4. No painel **Detalhes** da guia **capacidade**, na seção outros detalhes, clique no link ao lado de **cópias instantâneas**.

O número de cópias Snapshot é um link que exibe a lista de cópias snapshot.

### Informações relacionadas

["Página de integridade/volumes"](#)

## Exclusão de cópias Snapshot

Você pode excluir uma cópia Snapshot para economizar espaço ou liberar espaço em disco, ou excluir a cópia Snapshot se ela não for mais necessária.

### Antes de começar

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

O volume deve estar online.

Para excluir uma cópia Snapshot ocupada ou bloqueada, você deve ter liberado a cópia Snapshot do aplicativo que a estava usando.

- Não é possível excluir a cópia Snapshot base em um volume pai se um volume FlexClone estiver usando essa cópia Snapshot.

A cópia Snapshot de base é a cópia Snapshot usada para criar o volume FlexClone e exibe o status `Busy` e a dependência do aplicativo como `Busy`, `Vclone` no volume pai.

- Não é possível excluir uma cópia Snapshot bloqueada usada em uma relação do SnapMirror.

A cópia Snapshot está bloqueada e é necessária para a próxima atualização.

## Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. Na exibição **Saúde: Todos os volumes**, selecione o volume que contém as cópias Snapshot que deseja exibir.

A lista de cópias Snapshot é exibida.

3. Na página de detalhes **volume / Saúde**, clique na guia **capacidade**.
4. No painel **Detalhes** da guia **capacidade**, na seção outros detalhes, clique no link ao lado de **cópias instantâneas**.

O número de cópias Snapshot é um link que exibe a lista de cópias snapshot.

5. No modo de exibição **cópias Snapshot**, selecione as cópias Snapshot que deseja excluir e clique em **Excluir selecionadas**.

## Cálculo do espaço que pode ser recuperado para cópias Snapshot

Você pode calcular a quantidade de espaço em disco que pode ser recuperado se uma ou mais cópias Snapshot forem excluídas.

### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- O volume deve estar online.
- O volume deve ser um FlexVol volume; essa funcionalidade não é compatível com volumes FlexGroup.

## Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. Na exibição **Saúde: Todos os volumes**, selecione o volume que contém as cópias Snapshot que deseja exibir.

A lista de cópias Snapshot é exibida.

3. Na página de detalhes **volume / Saúde**, clique na guia **capacidade**.
4. No painel **Detalhes** da guia **capacidade**, na seção outros detalhes, clique no link ao lado de **cópias instantâneas**.

O número de cópias Snapshot é um link que exibe a lista de cópias snapshot.

5. Na exibição **cópias Snapshot**, selecione as cópias Snapshot para as quais você deseja calcular o espaço que pode ser recuperado.
6. Clique em **calcular**.

O espaço rereclamável (em porcentagem e KB, MB, GB e assim por diante) no volume é exibido.

7. Para recalcular o espaço que pode ser recuperado, selecione as cópias Snapshot necessárias e clique em **Recalcular**.

## Descrição das janelas de objetos de cluster e caixas de diálogo

É possível exibir todos os clusters e objetos de cluster na respectiva página de objetos de storage. Você também pode visualizar os detalhes na página de detalhes do objeto de armazenamento correspondente. Agora você pode iniciar a interface de usuário do System Manager nas seguintes seções DE ARMAZENAMENTO e PROTEÇÃO DO INVENTÁRIO.

- Páginas de inventário de cluster, integridade de cluster e desempenho de cluster
- Agregue as páginas de inventário, integridade agregada e desempenho agregado
- Páginas de inventário de volume, volume Health e volume Performance
- Páginas de inventário de nós e desempenho de nós
- Páginas de inventário do StorageVM, integridade do StorageVM e desempenho do StorageVM
- Páginas de relacionamento de proteção

## Tarefas e workflows de integridade do Unified Manager comuns

Alguns fluxos de trabalho administrativos e tarefas comuns associados ao Unified Manager incluem a seleção dos clusters de storage que devem ser monitorados; o diagnóstico de condições que afetam negativamente a disponibilidade, a capacidade e a proteção dos dados; a restauração de dados perdidos; a configuração e o gerenciamento de volumes; e o agrupamento e o envio de dados de diagnóstico para o suporte técnico (quando necessário).

Com o Unified Manager, os administradores de storage podem visualizar um dashboard, avaliar a capacidade geral, a disponibilidade e a integridade de proteção dos clusters de storage gerenciado e identificar, localizar, diagnosticar e atribuir rapidamente problemas específicos que possam surgir.

Os problemas mais importantes relacionados a um cluster, máquina virtual de armazenamento (SVM), volume ou volume FlexGroup que afetam a capacidade de armazenamento ou a disponibilidade de dados de seus objetos de armazenamento gerenciados são exibidos nos gráficos e eventos de integridade do sistema na página Painel. Quando problemas críticos são identificados, esta página fornece links para suportar fluxos de trabalho de solução de problemas apropriados.

O Unified Manager também pode ser incluído em fluxos de trabalho que incluem ferramentas de gerenciamento relacionadas, como o OnCommand Workflow Automation (WFA), para oferecer suporte à configuração direta de recursos de storage.

Fluxos de trabalho comuns relacionados às seguintes tarefas administrativas são descritos neste documento:

- Diagnosticar e gerenciar problemas de disponibilidade

Se problemas de configuração de recursos de armazenamento ou falha de hardware causarem a exibição de eventos de disponibilidade de dados na página Painel, os administradores de armazenamento podem seguir os links incorporados para exibir informações de conectividade sobre o recurso de armazenamento afetado, exibir conselhos de solução de problemas e atribuir resolução de problemas a outros administradores.

- Configuração e monitoramento de incidentes de desempenho

O administrador pode monitorar e gerenciar o desempenho dos recursos do sistema de armazenamento que estão sendo monitorados. Consulte ["Introdução ao monitoramento de desempenho do Active IQ Unified Manager"](#) para obter mais informações.

- Diagnósticos e gerenciamento de problemas de capacidade de volume

Se os problemas de capacidade de armazenamento de volume forem exibidos na página Painel, os administradores de armazenamento poderão seguir os links incorporados para exibir as tendências atuais e históricas relacionadas à capacidade de armazenamento do volume afetado, exibir conselhos de solução de problemas e atribuir resolução de problemas a outros administradores.

- Configuração, monitoramento e diagnóstico de problemas de relacionamento de proteção

Depois de criar e configurar relações de proteção, os administradores de armazenamento podem visualizar os potenciais problemas relacionados às relações de proteção, o estado atual das relações de proteção, as informações de sucesso do trabalho de proteção atual e histórico sobre as relações afetadas e conselhos para resolução de problemas. Consulte ["Criação, monitoramento e solução de problemas de relacionamentos de proteção"](#) para obter mais informações.

- Criar arquivos de backup e restaurar dados de arquivos de backup.
- Associar objetos de armazenamento a anotações

Ao associar objetos de storage a anotações, os administradores de storage podem filtrar e exibir os eventos relacionados aos objetos de storage, o que permite que os administradores de storage priorizem e resolvam os problemas associados aos eventos.

- Uso de APIs REST para ajudar a gerenciar clusters visualizando as informações de integridade, capacidade e desempenho capturadas pelo Unified Manager. Consulte ["Primeiros passos com as APIs REST do Active IQ Unified Manager"](#) para obter mais informações.
- Envio de um pacote de suporte ao suporte técnico

Os administradores de armazenamento podem recuperar e enviar um pacote de suporte ao suporte técnico usando o console de manutenção. Os pacotes de suporte devem ser enviados para o suporte técnico quando o problema exigir diagnóstico e solução de problemas mais detalhados do que o que uma mensagem do AutoSupport fornece.

## **Monitoramento e solução de problemas de disponibilidade de dados**

O Unified Manager monitora a confiabilidade com a qual os usuários autorizados podem acessar seus dados armazenados, emite alertas sobre condições que bloqueiam ou impedem esse acesso e permite diagnosticar essas condições e atribuir e rastrear sua resolução.

Os tópicos de fluxo de trabalho de disponibilidade nesta seção descrevem exemplos de como um administrador de storage pode usar a IU da Web do Unified Manager para descobrir, diagnosticar e atribuir para resolução condições de hardware e software que afetam negativamente a disponibilidade dos dados.

### **Verificação e resolução de condições de link de interconexão de failover de armazenamento**

Este fluxo de trabalho fornece um exemplo de como você pode procurar, avaliar e


resolver condições de link de interconexão de failover de armazenamento downed. Nesse cenário, você é um administrador que usa o Unified Manager para procurar riscos de failover de storage antes de iniciar uma atualização da versão do ONTAP nos nós.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Se as interconexões de failover de storage entre nós de par de HA falharem durante uma tentativa de atualização sem interrupções, a atualização falhará. Portanto, a prática comum é que o administrador monitore e confirme a confiabilidade do failover de storage nos nós de cluster direcionados para atualização antes do início de uma atualização.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.
2. Na página de inventário **Gerenciamento de Eventos**, selecione **Eventos de disponibilidade ativa**.
3. Na parte superior da coluna **Event Management** Inventory page **Name**, clique  e insira \*failover na caixa de texto para limitar o evento a ser exibido para eventos relacionados ao failover de armazenamento.

Todos os eventos anteriores relacionados às condições de failover de armazenamento são exibidos.

Nesse cenário, o Unified Manager exibe o evento ""Storage failover Interconnect One or More Links Down"" em sua seção de incidentes de disponibilidade.

4. Se um ou mais eventos relacionados ao failover de armazenamento forem exibidos na página de inventário **Gerenciamento de Eventos**, execute as seguintes etapas:
  - a. Clique no link do título do evento para exibir os detalhes do evento para esse evento.

Neste exemplo, você clica no título do evento ""Storage failover Interconnect One or More Links Down"".

A página de detalhes do evento para esse evento é exibida.

- a. Na página de detalhes do evento, você pode executar uma ou mais das seguintes tarefas:
  - Reveja a mensagem de erro no campo causa e avalie o problema.
  - Atribua o evento a um administrador.
  - Confirme o evento.

### Informações relacionadas

["Página de detalhes do evento"](#)

["Funções e recursos de usuário do Unified Manager"](#)

### Execução de ações corretivas para links de interconexão de failover de storage

Ao exibir a página de detalhes do evento de um evento relacionado ao failover de armazenamento, você pode revisar as informações resumidas da página para determinar a urgência do evento, a possível causa do problema e a possível resolução do problema.

## Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Neste cenário de exemplo, o resumo de eventos fornecido na página de detalhes do evento contém as seguintes informações sobre a condição de inatividade do link de interconexão de failover de armazenamento:

```
Event: Storage Failover Interconnect One or More Links Down
```

```
Summary
```

```
Severity: Warning
```

```
State: New
```

```
Impact Level: Risk
```

```
Impact Area: Availability
```

```
Source: aardvark
```

```
Source Type: Node
```

```
Acknowledged By:
```

```
Resolved By:
```

```
Assigned To:
```

```
Cause: At least one storage failover interconnected link  
       between the nodes aardvark and bonobo is down.  
       RDMA interconnect is up (Link0 up, Link1 down)
```

As informações de evento de exemplo indicam que um link de interconexão de failover de armazenamento, Link1, entre nós de par HA aardvark e bonobo está inativo, mas que link0 entre Apple e Boy está ativo. Como um link está ativo, o RDMA (Acesso remoto à memória dinâmica) ainda está funcionando e uma tarefa de failover de armazenamento ainda pode ser bem-sucedida.

No entanto, para garantir que a proteção contra falha de links e o failover de armazenamento seja totalmente desativado, você decide diagnosticar ainda mais o motivo da queda do Link1.

## Passos

1. Na página de detalhes **evento**, você pode clicar no link para o evento especificado no campo origem para obter mais detalhes sobre outros eventos que podem estar relacionados à condição de conexão de failover de armazenamento.

Neste exemplo, a fonte do evento é o nó chamado aardvark. Clicar nesse nome de nó exibe os Detalhes de HA para o par de HA afetado, aardvark e bonobo, na guia nós da página Detalhes de Cluster/Health e exibe outros eventos que ocorreram recentemente no par de HA afetado.

2. Consulte os **Detalhes HA** para obter mais informações sobre o evento.

Neste exemplo, as informações relevantes estão na tabela Eventos. A tabela mostra o evento "Storage failover Connection One or More Link Down", o tempo em que o evento foi gerado e, novamente, o nó a partir do qual este evento se originou.

Uso das informações de localização dos nós nos Detalhes da HA, solicitação ou conclusão pessoal de uma inspeção física e reparo do problema de failover de storage nos nós de par de HA afetados.

## Informações relacionadas

["Página de detalhes do evento"](#)

["Funções e recursos de usuário do Unified Manager"](#)

## Resolver problemas offline de volume

Esse fluxo de trabalho fornece um exemplo de como você pode avaliar e resolver um evento off-line de volume que o Unified Manager pode exibir na página de inventário do Gerenciamento de Eventos. Nesse cenário, você é um administrador usando o Unified Manager para solucionar problemas de um ou mais eventos offline de volume.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Os volumes podem ser reportados offline por várias razões:

- O administrador do SVM deliberadamente deixou o volume off-line.
- O nó de cluster de hospedagem do volume está inativo e o failover de storage para seu parceiro de par de HA também falhou.
- O volume que hospeda a máquina virtual de storage (SVM) é interrompido porque o nó que hospeda o volume raiz desse SVM está inativo.
- O agregado de hospedagem do volume está inativo devido a falha simultânea de dois discos RAID.

Você pode usar a página de inventário de Gerenciamento de Eventos e as páginas de detalhes de Cluster/Health, Storage VM/Health e volume/Health para confirmar ou eliminar uma ou mais dessas possibilidades.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.
2. Na página de inventário **Gerenciamento de Eventos**, selecione **Eventos de disponibilidade ativa**.
3. Clique no link de hipertexto exibido para o evento volume Offline.

A página de detalhes do evento para o incidente de disponibilidade é exibida.

4. Nessa página, verifique as notas para obter qualquer indicação de que o administrador da SVM colocou o volume em questão offline.
5. Na página de detalhes do **evento**, você pode revisar as informações de uma ou mais das seguintes tarefas:

- Reveja as informações apresentadas no campo de causa para obter instruções de diagnóstico possíveis.

Neste exemplo, as informações no campo causa informam apenas que o volume está offline.

- Verifique a área Notas e atualizações para obter qualquer indicação de que o administrador da SVM deliberadamente retirou o volume em questão offline.
- Clique na origem do evento, neste caso o volume que é relatado off-line, para obter mais informações sobre esse volume.
- Atribua o evento a um administrador.
- Reconheça o evento ou, se for o caso, marque-o como resolvido.



## Executar ações de diagnóstico para condições off-line de volume

Depois de navegar para a página de detalhes de volume / Saúde de um volume relatado estar offline, você pode procurar informações adicionais úteis para diagnosticar a condição offline do volume.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Se o volume que é relatado off-line não foi colocado off-line deliberadamente, esse volume pode estar off-line por vários motivos.

A partir da página de detalhes de volume/Saúde do volume offline, pode navegar para outras páginas e painéis para confirmar ou eliminar possíveis causas:

- Clique nos links da página de detalhes de **volume / Saúde** para determinar se o volume está off-line porque seu nó de host está inativo e o failover de armazenamento para seu parceiro de par de HA também falhou.

["Determinando se uma condição offline de volume é causada por um nó inativo"](#)Consulte .

- Clique nos links da página de detalhes de **volume / Saúde** para determinar se o volume está off-line e sua máquina virtual de armazenamento de host (SVM) é interrompida porque o nó que hospeda o volume raiz desse SVM está inativo.

["Determinando se um volume está off-line e o SVM é interrompido porque um nó está inativo"](#)Consulte .

- Clique nos links da página de detalhes de **volume / Saúde** para determinar se o volume está off-line devido a discos quebrados em seu agregado de host.

["Determinando se um volume está offline por causa de discos quebrados em um agregado"](#)Consulte .

### Informações relacionadas

["Funções e recursos de usuário do Unified Manager"](#)

### Determinando se um volume está offline porque seu nó de host está inativo

Você pode usar a IU da Web do Unified Manager para confirmar ou eliminar a possibilidade de um volume estar offline porque o nó do host está inativo e o failover de storage para seu parceiro de par de HA não tem êxito.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Para determinar se a condição de volume off-line é causada por falha do nó de hospedagem e subsequente failover de armazenamento mal-sucedido, execute as seguintes ações:

### Passos

1. Localize e clique no link de hipertexto exibido em SVM no painel **Related Devices** da página de detalhes **volume / Saúde** do volume off-line.

A página de detalhes da VM de armazenamento / integridade exibe informações sobre a máquina virtual


de armazenamento de hospedagem (SVM) do volume off-line.

2. No painel **Related Devices** (dispositivos relacionados) da página **Storage VM / Health details** (Detalhes da VM de armazenamento / Saúde)\*, localize e clique no link de hipertexto exibido em volumes.

A exibição integridade: Todos os volumes exibe uma tabela de informações sobre todos os volumes hospedados pelo SVM.

3. No cabeçalho da coluna Estado de exibição **Saúde: Todos os volumes**, clique no símbolo do filtro  e selecione a opção **Offline**.

Somente os volumes SVM que estão no estado offline são listados.

4. Na exibição Saúde: Todos os volumes, clique no símbolo de grade  e selecione a opção **Cluster Nodes**.

Talvez seja necessário rolar na caixa de seleção de grade para localizar a opção **Cluster Nodes**.

A coluna Cluster Nodes é adicionada ao inventário de volumes e exibe o nome do nó que hospeda cada volume off-line.

5. Na exibição **Saúde: Todos os volumes**, localize a listagem do volume off-line e, em sua coluna Cluster Node, clique no nome de seu nó de hospedagem.

A guia nós na página Detalhes do cluster / integridade exibe o estado do par de nós de HA ao qual o nó de hospedagem pertence. O estado do nó de hospedagem e o sucesso de qualquer operação de failover de cluster são indicados no visor.

Depois de confirmar que a condição de volume off-line existe porque o nó de host está inativo e o failover de armazenamento para o parceiro de par de HA falhou, entre em Contato com o administrador ou operador apropriado para reiniciar manualmente o nó de entrada e corrigir o problema de failover de armazenamento.

### **Determinando se um volume está off-line e sua SVM é interrompida porque um nó está inativo**

Você pode usar a IU da Web do Unified Manager para confirmar ou eliminar a possibilidade de um volume ficar off-line, pois sua máquina virtual de storage de host (SVM) é interrompida devido ao nó que hospeda o volume raiz desse SVM estar inativo.

#### **Antes de começar**

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.


Para determinar se a condição de volume off-line está interrompida porque o nó que hospeda o volume raiz do SVM está inativo, execute as seguintes ações:

#### **Passos**

1. Localize e clique no link de hipertexto exibido sob o SVM no painel **Related Devices** da página de detalhes **volume / Saúde** do volume off-line.

A página de detalhes da VM de armazenamento / integridade exibe o status "em execução" ou "coberto" do SVM de hospedagem. Se o status SVM estiver em execução, a condição de volume off-line não será causada pelo nó que hospeda o volume raiz do SVM inativo.

2. Se o status SVM for interrompido, clique em **Exibir SVMs** para identificar ainda mais a causa da interrupção do SVM de hospedagem.

3. No cabeçalho da coluna **Health: All Storage VMs** view SVM, clique no símbolo de filtro  e digite o nome do SVM parado.

As informações desse SVM são mostradas em uma tabela.

4. Na exibição **Saúde: Todas as VMs de armazenamento**, clique  e selecione a opção **volume raiz**.

A coluna volume raiz é adicionada ao inventário SVM e exibe o nome do volume raiz do SVM parado.

5. Na coluna volume raiz, clique no nome do volume raiz para exibir a página de detalhes **Storage VM / Health** para esse volume.

Se o status do volume raiz do SVM for (Online), a condição de volume off-line original não será causada porque o nó que hospeda o volume raiz desse SVM está inativo.

6. Se o status do volume raiz do SVM for (Offline), localize e clique no link de hipertexto exibido em agregar no painel dispositivos relacionados da página de detalhes volume/integridade do volume raiz SVM.
7. Localize e clique no link de hipertexto exibido em nó no painel **Related Devices** da página de detalhes **Advertment / Health** do agregado.

A guia nós na página de detalhes de cluster/integridade exibe o estado do par de nós de HA ao qual pertence o nó de hospedagem do volume raiz SVM. O estado do nó é indicado no visor.

Depois de confirmar que a condição de volume off-line é causada pela condição off-line SVM do host desse volume, o que por si só é causado pelo nó que hospeda o volume raiz do SVM inativo, entre em Contato com o administrador ou operador apropriado para reiniciar manualmente o nó inativo.

### **Determinando se um volume está offline por causa de discos quebrados em um agregado**

Você pode usar a IU da Web do Unified Manager para confirmar ou eliminar a possibilidade de um volume estar offline porque os problemas de disco RAID tornaram seu agregado de host offline.

#### **Antes de começar**

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Para determinar se a condição off-line do volume é causada por problemas de disco RAID que estão tomando o agregado de hospedagem offline, execute as seguintes ações:

#### **Passos**

1. Localize e clique no link de hipertexto exibido em agregado no painel **Related Devices** da página de detalhes **volume / Saúde**.

A página de detalhes de agregado / Saúde exibe o status online ou offline do agregado de hospedagem. Se o status agregado estiver on-line, os problemas do disco RAID não são a causa do volume estar off-line.

2. Se o status agregado estiver offline, clique em **informações do disco** e procure eventos de disco quebrados na lista **Eventos** na guia **informações do disco**.
3. Para identificar ainda mais os discos quebrados, clique no link de hipertexto exibido em Node no painel **Related Devices** (dispositivos relacionados).

É apresentada a página Cluster / Health details (Detalhes do Cluster/Health).

4. Clique em **Disks** e selecione **Broken** no painel **Filters** para listar todos os discos no estado quebrado.

Se os discos no estado quebrado causarem o estado offline do agregado de host, o nome do agregado será exibido na coluna agregado impactado.

Depois de confirmar que a condição de volume off-line é causada por discos RAID quebrados e o consequente agregado de host off-line, entre em Contato com o administrador ou operador apropriado para substituir manualmente os discos quebrados e colocar o agregado de volta on-line.

## Resolução de problemas de capacidade

Este fluxo de trabalho fornece um exemplo de como você pode resolver um problema de capacidade. Nesse cenário, você é um administrador ou operador e acessa a página do Unified ManagerDashboard para ver se algum dos objetos de storage monitorados tem problemas de capacidade. Você deseja determinar a possível causa e resolução do problema.

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Na página Painel, você procura um evento de erro ""espaço de volume cheio"" no painel capacidade na lista suspensa eventos.

### Passos

1. No painel **Capacity** da página **Dashboard**, clique no nome do evento de erro espaço em volume cheio.

A página de detalhes do evento para o erro é exibida.

2. Na página de detalhes do **evento**, você pode executar uma ou mais das seguintes tarefas:

- Reveja a mensagem de erro no campo causa e clique nas sugestões em ações corretivas sugeridas para rever as descrições de possíveis correções.
- Clique no nome do objeto, neste caso um volume, no campo fonte para obter detalhes sobre o objeto.
- Procure por notas que possam ter sido adicionadas sobre este evento.
- Adicione uma nota ao evento.
- Atribua o evento a outro usuário.
- Confirme o evento.
- Marque o evento como resolvido.

### Informações relacionadas

["Página de detalhes do evento"](#)

### Executar ações corretivas sugeridas para um volume total

Depois de receber um evento de erro "volume Space Full", você analisa as ações corretivas sugeridas na página de detalhes do evento e decide executar uma das ações sugeridas.

### Antes de começar

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

Um usuário com qualquer função pode executar todas as tarefas desse fluxo de trabalho que usam o Unified Manager.

Neste exemplo, você viu um evento de erro espaço de volume cheio na página de inventário do Unified Manager Event Management e clicou no nome do evento.

As possíveis ações corretivas que você pode executar para um volume completo incluem as seguintes:

- Habilitando o crescimento automático, a deduplicação ou a compactação no volume
- Redimensionar ou mover o volume
- Eliminar ou mover dados do volume

Embora todas essas ações devam ser executadas no Gerenciador do sistema do ONTAP ou na CLI do ONTAP, você pode usar o Gerenciador unificado para encontrar informações necessárias para determinar quais ações tomar.

### Passos

1. Na página de detalhes do **evento**, clique no nome do volume no campo origem para exibir detalhes sobre o volume afetado.
2. Na página de detalhes **volume / Saúde**, você clica em **Configuração** e vê que a deduplicação e a compactação já estão ativadas no volume.

Você decide redimensionar o volume.

3. No painel **Related Devices** (dispositivos relacionados), clique no nome do agregado de hospedagem para ver se o agregado pode acomodar um volume maior.
4. Na página de detalhes **agregado / Saúde**, você vê que o agregado que hospeda o volume total tem capacidade não comprometida suficiente, então você usa o Gerenciador de sistema ONTAP para redimensionar o volume, dando mais capacidade.

### Informações relacionadas

["Página de detalhes do evento"](#)

## Gerenciamento de limites de integridade

Você pode configurar valores de limite de integridade globais para todos os agregados, volumes e qtrees para rastrear quaisquer violações de limites de integridade.

### Quais são os limites de integridade da capacidade de storage

Um limite de integridade da capacidade de storage é o ponto em que o servidor do Unified Manager gera eventos para relatar qualquer problema de capacidade com objetos de storage. Você pode configurar alertas para enviar notificações sempre que tais eventos ocorrerem.

Os limites de integridade da capacidade de storage para todos os agregados, volumes e qtrees são definidos como valores padrão. Você pode alterar as configurações conforme necessário para um objeto ou um grupo de objetos.

## Configurar definições de limites globais de saúde

Você pode configurar condições de limite de integridade globais para capacidade, crescimento, reserva de snapshot, cotas e inodes para monitorar seu agregado, volume e tamanho de qtree com eficiência. Você também pode editar as configurações para gerar eventos para exceder limites de atraso.

As configurações de limites globais de integridade se aplicam a todos os objetos aos quais estão associados, como agregados, volumes, etc. Quando os limites são cruzados, um evento é gerado e, se os alertas forem configurados, uma notificação de alerta é enviada. Os padrões de limite são definidos como valores recomendados, mas você pode modificá-los para gerar eventos em intervalos para atender às suas necessidades específicas. Quando os limites são alterados, os eventos são gerados ou obsoletos no próximo ciclo de monitoramento.

As definições de limites globais de saúde estão acessíveis a partir da seção limites de eventos do menu de navegação à esquerda. Você também pode modificar as configurações de limite para objetos individuais, a partir da página de inventário ou da página de detalhes para esse objeto.

- Para obter informações, "[Configurando valores de limite globais de integridade agregada](#)" consulte .

Você pode configurar as configurações de limite de integridade para capacidade, crescimento e cópias Snapshot de todos os agregados para controlar qualquer violação de limite.

- Para obter informações, "[Configuração dos valores do limite de integridade do volume global](#)" consulte .

Você pode editar as configurações de limite de integridade para capacidade, cópias Snapshot, cotas de qtree, crescimento de volume, sobrescrever espaço de reserva e inodes para todos os volumes para controlar qualquer violação de limite.

- Para obter informações, "[Configurando valores de limite de integridade de qtree global](#)" consulte .

Você pode editar as configurações de limite de integridade para a capacidade de todos os qtrees para rastrear qualquer violação de limite.

- Para obter informações, "[Editar as configurações de limite de integridade de atraso para relacionamentos de proteção não gerenciados](#)" consulte .

Você pode aumentar ou diminuir a porcentagem de tempo de atraso de aviso ou erro para que os eventos sejam gerados em intervalos mais adequados às suas necessidades.

### Configurando valores de limite globais de integridade agregada

Você pode configurar valores de limite de integridade globais para todos os agregados para rastrear qualquer violação de limite. Eventos apropriados são gerados para violações de limites e você pode tomar medidas preventivas com base nesses eventos. Você pode configurar os valores globais com base nas configurações de práticas recomendadas para limites que se aplicam a todos os agregados monitorados.

#### Antes de começar

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

Quando você configura as opções globalmente, os valores padrão dos objetos são modificados. No entanto, se os valores padrão tiverem sido alterados no nível do objeto, os valores globais não serão modificados.

As opções de limite têm valores padrão para melhor monitoramento, no entanto, você pode alterar os valores de acordo com os requisitos do seu ambiente.

Quando o crescimento automático é ativado em volumes que residem no agregado, os limites de capacidade agregada são considerados violados com base no tamanho máximo do volume definido pelo crescimento automático, não com base no tamanho do volume original.



Os valores de limite de integridade não são aplicáveis ao agregado raiz do nó.

### Passos

1. No painel de navegação à esquerda, clique em **limites de eventos > agregado**.
2. Configurar os valores-limite apropriados para capacidade, crescimento e cópias Snapshot.
3. Clique em **Salvar**.

### Informações relacionadas

["Adicionando usuários"](#)

#### Configuração dos valores do limite de integridade do volume global

Você pode configurar os valores de limite de integridade global para todos os volumes para rastrear qualquer violação de limite. Eventos apropriados são gerados para violações de limites de integridade e você pode tomar medidas preventivas com base nesses eventos. Você pode configurar os valores globais com base nas configurações de práticas recomendadas para limites que se aplicam a todos os volumes monitorados.

#### Antes de começar

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

A maioria das opções de limite tem valores padrão para melhor monitoramento. No entanto, você pode alterar os valores de acordo com os requisitos do seu ambiente.

Observe que, quando o crescimento automático está ativado em um volume, os limites de capacidade são considerados violados com base no tamanho máximo do volume definido pelo crescimento automático, não com base no tamanho do volume original.



O valor padrão de 1000 cópias Snapshot é aplicável somente a volumes FlexVol quando a versão do ONTAP é 9,4 ou superior e a volumes FlexGroup quando a versão do ONTAP é 9,8 ou superior. Para clusters instalados com versões mais antigas do software ONTAP, o número máximo é de 250 cópias de Snapshot por volume. Para essas versões mais antigas, o Unified Manager interpreta esse número 1000 (e qualquer número entre 1000 e 250) como 250; o que significa que você continuará recebendo eventos quando o número de cópias Snapshot chegar a 250. Se você deseja definir esse limite para menos de 250 para essas versões mais antigas, você deve definir o limite para 250 ou mais baixo aqui, na exibição Saúde: Todos os volumes ou na página Detalhes volume / Saúde.

### Passos

1. No painel de navegação esquerdo, clique em **limites de eventos > volume**.
2. Configurar os valores de limite apropriados para capacidade, cópias Snapshot, cotas de qtree, crescimento de volume e inodes.

3. Clique em **Salvar**.

## Informações relacionadas

["Adicionando usuários"](#)

### Configurando valores de limite de integridade de qtree global

Você pode configurar os valores de limite de integridade global para todos os qtrees para rastrear qualquer violação de limite. Eventos apropriados são gerados para violações de limites de integridade e você pode tomar medidas preventivas com base nesses eventos. Você pode configurar os valores globais com base nas configurações de práticas recomendadas para limites que se aplicam a todos os qtrees monitorados.

#### Antes de começar

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

As opções de limite têm valores padrão para melhor monitoramento, no entanto, você pode alterar os valores de acordo com os requisitos do seu ambiente.

Os eventos são gerados para uma qtree somente quando uma cota Qtree ou uma cota padrão tiver sido definida na qtree. Os eventos não são gerados se o espaço definido em uma cota de usuário ou cota de grupo tiver excedido o limite.

#### Passos

1. No painel de navegação esquerdo, clique em **limites de eventos > Qtree**.
2. Configure os valores de limite de capacidade apropriados.
3. Clique em **Salvar**.

### Configuração de configurações de limite de atraso para relacionamentos de proteção não gerenciados

Você pode editar as configurações de aviso de atraso padrão global e limite de integridade de erro para relacionamentos de proteção não gerenciados para que os eventos sejam gerados em intervalos adequados às suas necessidades.

#### Antes de começar

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

O tempo de atraso não deve ser superior ao intervalo de programação de transferência definido. Por exemplo, se o agendamento de transferência for de hora em hora, o tempo de atraso não deve ser superior a uma hora. O limite de atraso especifica uma porcentagem que o tempo de atraso não deve exceder. Usando o exemplo de uma hora, se o limite de atraso for definido como 150%, você receberá um evento quando o tempo de atraso for superior a 1,5 horas.

As configurações descritas nesta tarefa são aplicadas globalmente a todos os relacionamentos de proteção não gerenciados. As configurações não podem ser especificadas e aplicadas exclusivamente a uma relação de proteção não gerenciada.

#### Passos

1. No painel de navegação à esquerda, clique em **limites de eventos > relacionamento**.
2. Aumente ou diminua a porcentagem de tempo de atraso de aviso ou erro padrão global, conforme



necessário.

3. Para desativar o acionamento de um evento de aviso ou erro a partir de qualquer valor limite de atraso, desmarque a caixa ao lado de **Enabled**.
4. Clique em **Salvar**.

## Informações relacionadas

["Adicionando usuários"](#)

### Editar configurações individuais de limite de integridade agregado

Você pode editar as configurações de limite de integridade para capacidade agregada, crescimento e cópias Snapshot de um ou mais agregados. Quando um limite é cruzado, os alertas são gerados e você recebe notificações. Essas notificações ajudam você a tomar medidas preventivas com base no evento gerado.

#### Antes de começar

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

Com base nas alterações nos valores de limite, os eventos são gerados ou obsoletos no próximo ciclo de monitoramento.

Quando o crescimento automático é ativado em volumes que residem no agregado, os limites de capacidade agregada são considerados violados com base no tamanho máximo do volume definido pelo crescimento automático, não com base no tamanho do volume original.

#### Passos

1. No painel de navegação à esquerda, clique em **Storage > Aggregates**.
2. Na exibição **Saúde: Todos os agregados**, selecione um ou mais agregados e clique em **Editar limites**.
3. Na caixa de diálogo **Editar limites agregados**, edite as configurações de limite de uma das seguintes opções: Capacidade, crescimento ou cópias Snapshot selecionando a caixa de seleção apropriada e modificando as configurações.
4. Clique em **Salvar**.

## Informações relacionadas

["Adicionando usuários"](#)

### Editar definições individuais de limite de integridade do volume

Você pode editar as configurações de limite de integridade para capacidade de volume, crescimento, cota e reserva de espaço de um ou mais volumes. Quando um limite é cruzado, os alertas são gerados e você recebe notificações. Essas notificações ajudam você a tomar medidas preventivas com base no evento gerado.

#### Antes de começar

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

Com base nas alterações nos valores de limite, os eventos são gerados ou obsoletos no próximo ciclo de monitoramento.

Observe que, quando o crescimento automático está ativado em um volume, os limites de capacidade são considerados violados com base no tamanho máximo do volume definido pelo crescimento automático, não com base no tamanho do volume original.



O valor padrão de 1000 cópias Snapshot é aplicável somente a volumes FlexVol quando a versão do ONTAP é 9,4 ou superior e a volumes FlexGroup quando a versão do ONTAP é 9,8 ou superior. Para clusters instalados com versões mais antigas do software ONTAP, o número máximo é de 250 cópias de Snapshot por volume. Para essas versões mais antigas, o Unified Manager interpreta esse número 1000 (e qualquer número entre 1000 e 250) como 250; o que significa que você continuará recebendo eventos quando o número de cópias Snapshot chegar a 250. Se você deseja definir esse limite para menos de 250 para essas versões mais antigas, você deve definir o limite para 250 ou mais baixo aqui, na exibição Saúde: Todos os volumes ou na página Detalhes volume / Saúde.

## Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. Na exibição **Saúde: Todos os volumes**, selecione um ou mais volumes e clique em **Editar limites**.
3. Na caixa de diálogo **Editar limites de volume**, edite as configurações de limite de uma das seguintes opções: Capacidade, cópias Snapshot, cota de qtree, crescimento ou inodes selecionando a caixa de seleção apropriada e modificando as configurações.
4. Clique em **Salvar**.

## Informações relacionadas

["Adicionando usuários"](#)

## Editar configurações individuais de limite de integridade de qtree

Você pode editar as configurações de limite de integridade para a capacidade de qtree para um ou mais qtrees. Quando um limite é cruzado, os alertas são gerados e você recebe notificações. Essas notificações ajudam você a tomar medidas preventivas com base no evento gerado.

### Antes de começar

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

Com base nas alterações nos valores de limite, os eventos são gerados ou obsoletos no próximo ciclo de monitoramento.

## Passos

1. No painel de navegação esquerdo, clique em **Storage > Qtrees**.
2. Na visualização **Capacity: All Qtrees**, selecione um ou mais qtrees e clique em **Edit thresholds**.
3. Na caixa de diálogo **Editar limites de Qtree**, altere os limites de capacidade para a qtree ou qtrees selecionados e clique em **Salvar**.



Você também pode definir limites de qtree individuais na guia Qtrees na página Storage VM / Health details.

## Gerenciamento dos objetivos de segurança do cluster

O Unified Manager fornece um dashboard que identifica a segurança dos clusters do ONTAP, das máquinas virtuais de storage (SVMs) e dos volumes com base nas recomendações definidas no *Guia de endurecimento de segurança do NetApp para ONTAP 9*.

O objetivo do dashboard de segurança é mostrar todas as áreas em que os clusters do ONTAP não estejam alinhados às diretrizes recomendadas do NetApp para que você possa corrigir esses possíveis problemas. Na maioria dos casos, você corrigirá os problemas usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP. Sua organização pode não seguir todas as recomendações, então, em alguns casos, você não precisará fazer alterações.

Consulte o "[Guia de endurecimento de segurança da NetApp para ONTAP 9](#)" (TR-4569) para obter recomendações e resoluções detalhadas.

Além de informar o status de segurança, o Unified Manager também gera eventos de segurança para qualquer cluster ou SVM que tenha violações de segurança. Você pode rastrear esses problemas na página de inventário do Gerenciamento de Eventos e configurar alertas para esses eventos para que o administrador de armazenamento seja notificado quando novos eventos de segurança ocorrerem.

Para obter mais informações, "[Quais critérios de segurança estão sendo avaliados](#)" consulte .

### Quais critérios de segurança estão sendo avaliados

Em geral, os critérios de segurança dos clusters do ONTAP, das máquinas virtuais de armazenamento (SVMs) e dos volumes estão sendo avaliados em relação às recomendações definidas no *Guia de endurecimento de Segurança do NetApp para ONTAP 9*.

Algumas das verificações de segurança incluem:

- Se um cluster está usando um método de autenticação seguro, como SAML
- se os clusters peered têm sua comunicação criptografada
- Se uma VM de storage tem seu log de auditoria habilitado
- se seus volumes têm criptografia de software ou hardware ativada

Consulte os tópicos sobre categorias de conformidade e o "[Guia de endurecimento de segurança da NetApp para ONTAP 9](#)" para obter informações detalhadas.



Os eventos de atualização que são relatados da plataforma Active IQ também são considerados eventos de segurança. Esses eventos identificam problemas em que a resolução exige que você atualize o software ONTAP, o firmware do nó ou o software do sistema operacional (para avisos de segurança). Esses eventos não são exibidos no painel Segurança, mas estão disponíveis na página de inventário do Gerenciamento de Eventos.

Para obter mais informações, "[Gerenciamento dos objetivos de segurança do cluster](#)" consulte .

### Categorias de conformidade de cluster

Esta tabela descreve os parâmetros de conformidade de segurança do cluster que o

Unified Manager avalia, a recomendação do NetApp e se o parâmetro afeta a determinação geral do cluster que está sendo queixa ou não.

Ter SVMs não compatíveis em um cluster afetará o valor de conformidade do cluster. Então, em alguns casos, você pode precisar corrigir problemas de segurança com um SVM antes que a segurança do cluster seja considerada em conformidade.

Note que nem todos os parâmetros listados abaixo aparecem para todas as instalações. Por exemplo, se você não tiver clusters com peering ou se tiver desabilitado o AutoSupport em um cluster, não verá os itens de emparelhamento de cluster ou Transporte HTTPS AutoSupport na página da IU.

<b>Parâmetro</b>	<b>Descrição</b>	<b>Recomendação</b>	<b>Afeta a conformidade do cluster</b>
FIPS global	Indica se o modo de conformidade Global FIPS (Federal Information Processing Standard) 140-2 está ativado ou desativado. Quando o FIPS está ativado, TLSv1 e SSLv3 são desativados e apenas TLSv1,1 e TLSv1,2 são permitidos.	Ativado	Sim
Telnet	Indica se o acesso Telnet ao sistema está ativado ou desativado. A NetApp recomenda o Shell seguro (SSH) para acesso remoto seguro.	Desativado	Sim
Configurações SSH inseguras	Indica se o SSH usa cifras inseguras, por exemplo cifras que começam com *cbc.	Não	Sim
Banner de login	Indica se o banner Login está ativado ou desativado para os usuários que acessam o sistema.	Ativado	Sim

<b>Parâmetro</b>	<b>Descrição</b>	<b>Recomendação</b>	<b>Afeta a conformidade do cluster</b>
Peering de clusters	Indica se a comunicação entre clusters com permissões está encriptada ou não encriptada. A criptografia deve ser configurada nos clusters de origem e destino para que esse parâmetro seja considerado compatível.	Encriptado	Sim
Protocolo de hora de rede	Indica se o cluster tem um ou mais servidores NTP configurados. Para redundância e melhor serviço, a NetApp recomenda que você associe pelo menos três servidores NTP ao cluster.	Configurado	Sim
OCSP	Indica se existem aplicações no ONTAP que não estão configuradas com OCSP (Protocolo de estado de certificado online) e, por conseguinte, as comunicações não estão encriptadas. As aplicações não compatíveis estão listadas.	Ativado	Não
Registo de auditoria remota	Indica se o encaminhamento de registos (Syslog) está encriptado ou não encriptado.	Encriptado	Sim
Transporte AutoSupport HTTPS	Indica se o HTTPS é usado como o protocolo de transporte padrão para enviar mensagens AutoSupport ao suporte do NetApp.	Ativado	Sim

<b>Parâmetro</b>	<b>Descrição</b>	<b>Recomendação</b>	<b>Afeta a conformidade do cluster</b>
Usuário Administrador padrão	Indica se o Usuário Admin padrão (interno) está ativado ou desativado. A NetApp recomenda bloquear (desativar) quaisquer contas internas desnecessárias.	Desativado	Sim
Usuários SAML	Indica se o SAML está configurado. O SAML permite configurar a autenticação multifator (MFA) como um método de login para logon único.	Não	Não
Usuários do ative Directory	Indica se o ative Directory está configurado. O ative Directory e o LDAP são os mecanismos de autenticação preferenciais para usuários que acessam clusters.	Não	Não
Utilizadores LDAP	Indica se o LDAP está configurado. O ative Directory e o LDAP são os mecanismos de autenticação preferidos para usuários que gerenciam clusters em usuários locais.	Não	Não
Usuários de certificados	Indica se um utilizador de certificado está configurado para iniciar sessão no cluster.	Não	Não
Usuários locais	Indica se os utilizadores locais estão configurados para iniciar sessão no cluster.	Não	Não

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
Shell remoto	Indica se o RSH está ativado. Por razões de segurança, o RSH deve ser desativado. O Secure Shell (SSH) para acesso remoto seguro é o preferido.	Desativado	Sim
MD5 em uso	Indica se as contas de usuário do ONTAP usam a função Hash MD5 menos segura. A migração de contas de usuário com hash MD5 para a função hash criptográfica mais segura, como SHA-512, é preferível.	Não	Sim
Tipo de emissor de certificado	Indica o tipo de certificado digital utilizado.	Assinado pela CA	Não

#### Categorias de conformidade de VM de storage

Esta tabela descreve os critérios de conformidade de segurança da máquina virtual de storage (SVM) avaliados pelo Unified Manager, a recomendação do NetApp e se o parâmetro afeta a determinação geral da reclamação ou não da SVM.

Parâmetro	Descrição	Recomendação	Diz respeito à conformidade com o SVM
Registo de auditoria	Indica se o registo de auditoria está ativado ou desativado.	Ativado	Sim
Configurações SSH inseguras	Indica se o SSH usa cifras inseguras, por exemplo, cifras que começam com <i>cbc*</i> .	Não	Sim
Banner de login	Indica se o banner Login está ativado ou desativado para usuários que acessam SVMs no sistema.	Ativado	Sim

<b>Parâmetro</b>	<b>Descrição</b>	<b>Recomendação</b>	<b>Diz respeito à conformidade com o SVM</b>
Encriptação LDAP	Indica se a encriptação LDAP está ativada ou desativada.	Ativado	Não
Autenticação NTLM	Indica se a autenticação NTLM está ativada ou desativada.	Ativado	Não
Assinatura de carga útil LDAP	Indica se a assinatura de carga útil LDAP está ativada ou desativada.	Ativado	Não
Definições CHAP	Indica se o CHAP está ativado ou desativado.	Ativado	Não
Kerberos V5	Indica se a autenticação Kerberos V5 está ativada ou desativada.	Ativado	Não
Autenticação NIS	Indica se o uso da autenticação NIS está configurado.	Desativado	Não
Estado FPolicy ativo	Indica se FPolicy foi criado ou não.	Sim	Não
Encriptação SMB ativada	Indica se SMB -assinatura e selagem não estão ativados.	Sim	Não
Assinatura SMB ativada	Indica se a assinatura SMB não está ativada.	Sim	Não

#### **Categorias de conformidade de volume**

Esta tabela descreve os parâmetros de criptografia de volume avaliados pelo Unified Manager para determinar se os dados nos volumes estão protegidos adequadamente contra o acesso de usuários não autorizados.

Observe que os parâmetros de criptografia de volume não afetam se o cluster ou a VM de armazenamento são considerados compatíveis.






Parâmetro	Descrição
Software criptografado	Exibe o número de volumes protegidos usando as soluções de criptografia de software de criptografia de volume NetApp (NVE) ou NetApp Aggregate Encryption (NAE).
Hardware criptografado	Exibe o número de volumes protegidos usando criptografia de hardware do NetApp Storage Encryption (NSE).
Software e hardware criptografados	Exibe o número de volumes protegidos pela criptografia de software e hardware.
Não encriptado	Exibe o número de volumes que não são criptografados.

### O que não está em conformidade significa

Os clusters e as máquinas virtuais de armazenamento (SVMs) são considerados não compatíveis quando nenhum dos critérios de segurança que está sendo avaliado em relação às recomendações definidas no *Guia de endurecimento de Segurança do NetApp para ONTAP 9* não for atendido. Além disso, um cluster é considerado não compatível quando qualquer SVM é sinalizado como não compatível.

Os ícones de status nos cartões de segurança têm os seguintes significados em relação à sua conformidade:

-  - O parâmetro é configurado como recomendado.
-  - O parâmetro não está configurado como recomendado.
-  - Ou a funcionalidade não está ativada no cluster, ou o parâmetro não está configurado como recomendado, mas este parâmetro não contribui para a conformidade do objeto.

Observe que o status de criptografia de volume não contribui para se o cluster ou SVM são considerados em conformidade.

### Visualização do status de segurança dos clusters e das VMs de storage

O Active IQ Unified Manager permite visualizar o status de segurança dos objetos de storage em seu ambiente a partir de diferentes pontos na interface. Você pode coletar e analisar informações e relatórios com base em parâmetros definidos e detectar comportamentos suspeitos ou alterações de sistema não autorizadas nos clusters monitorados e nas VMs de storage.

Para obter as recomendações de segurança, consulte a ["Guia de endurecimento de segurança da NetApp para ONTAP 9"](#)

### Exibir status de segurança no nível do objeto na página Segurança

Como administrador de sistema, você pode usar a página **Segurança** para obter visibilidade da força de

segurança dos clusters do ONTAP e das VMs de armazenamento nos níveis do data center e do local. Os objetos suportados são cluster, máquinas virtuais de storage e volumes. Siga estes passos:

### Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Dependendo se você deseja exibir o status de segurança para todos os clusters monitorados ou para um único cluster, selecione **todos os clusters** ou selecione um único cluster no menu suspenso.
3. Clique na seta para a direita no painel **Segurança**. É apresentada a página Segurança.

Clicar nos gráficos de barras, contagens e `View Reports` links leva você à página volumes, clusters ou VMs de armazenamento para que você possa visualizar os detalhes correspondentes ou gerar relatórios, conforme necessário.

A página Segurança exibe os seguintes painéis:

- **Cluster Compliance:** O status de segurança (número de clusters compatíveis ou não compatíveis) de todos os clusters em um data center
- **Storage VM Compliance:** O status de segurança (número de VMs de armazenamento compatíveis ou não compatíveis) para todas as VMs de armazenamento em seu data center
- **Criptografia de volume:** O status de criptografia de volume (número de volumes criptografados ou não criptografados) de todos os volumes em seu ambiente
- **Volume Anti-ransomware Status:** O status de segurança (número de volumes com anti-ransomware ativado ou desativado) de todos os volumes em seu ambiente
- **Autenticação de cluster e certificados:** O número de clusters que usam cada tipo de método de autenticação, como SAML, ative Directory ou por meio de certificados e autenticação local. O painel também exibe o número de clusters cujos certificados expiraram ou estão prestes a expirar em 60 dias.

### Veja os detalhes de segurança de todos os clusters na página clusters

A página de detalhes **clusters / Segurança** permite exibir o status de conformidade de segurança em um nível de cluster.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > clusters**.
2. Selecione **Exibir > Segurança > todos os clusters**.

Parâmetros de segurança padrão, como FIPS global, Telnet, configurações de SSH inseguras, banner de login, protocolo de tempo de rede, transporte HTTPS AutoSupport e o status da expiração do certificado de cluster são exibidos.

Você pode clicar no ⓘ botão mais opções e optar por exibir os detalhes de segurança na página **Segurança** do Unified Manager ou no System Manager. Você deve ter credenciais válidas para visualizar os detalhes no System Manager.



Se um cluster tiver um certificado expirado, você pode clicar `expired` em **validade do certificado de cluster** e renová-lo a partir do System Manager (9.10.1 e posterior). Não é possível clicar `expired` se a instância do System Manager for de uma versão anterior a 9.10.1.


## Veja os detalhes de segurança de todos os clusters na página de VMs de storage

A página de detalhes **Storage VMs / Security** permite que você visualize o status de conformidade de segurança em um nível de VM de armazenamento.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > Storage VMs**.
2. Selecione **Exibir > Segurança > todas as VMs de armazenamento**. É apresentada uma lista de clusters com os parâmetros de segurança.

Você pode ter uma visualização padrão da conformidade de segurança das VMs de armazenamento verificando os parâmetros de segurança, como VMs de armazenamento, cluster, banner de login, log de auditoria e configurações SSH inseguras.

Você pode clicar no  botão mais opções e optar por exibir os detalhes de segurança na página **Segurança** do Unified Manager ou no System Manager. Você deve ter credenciais válidas para visualizar os detalhes no System Manager.

Para obter detalhes de segurança contra ransomware para volumes e VMs de storage, "[Visualização do status anti-ransomware de todos os volumes e VMs de storage](#)" consulte .

## Exibição de eventos de segurança que podem exigir atualizações de software ou firmware

Existem certos eventos de segurança que têm uma área de impactos do "Upgrade". Esses eventos são relatados da plataforma Active IQ e identificam problemas em que a resolução exige que você atualize o software ONTAP, o firmware do nó ou o software do sistema operacional (para avisos de segurança).

### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Você pode querer executar ações corretivas imediatas para alguns desses problemas, enquanto outros problemas podem esperar até a próxima manutenção programada. Você pode visualizar todos esses eventos e atribuí-los a usuários que podem resolver os problemas. Além disso, se houver certos eventos de atualização de segurança sobre os quais você não deseja ser notificado, esta lista pode ajudá-lo a identificar esses eventos para que você possa desativá-los.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.

Por padrão, todos os eventos ativos (novos e confirmados) são exibidos na página de inventário do Gerenciamento de Eventos.

2. No menu Exibir, selecione **Atualizar eventos**.

A página exibe todos os eventos de segurança de atualização ativos.

## Visualização de como a autenticação do usuário está sendo gerenciada em todos os clusters

A página Segurança exibe os tipos de autenticação que estão sendo usados para autenticar usuários em cada cluster e o número de usuários que estão acessando o cluster usando cada tipo. Isso permite verificar se a autenticação do usuário está sendo

executada de forma segura, conforme definido pela sua organização.

### Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Na parte superior do painel, selecione **todos os clusters** no menu suspenso.
3. Clique na seta para a direita no painel **Segurança** e a página **Segurança** será exibida.
4. Exiba o cartão **Cluster Authentication** para ver o número de usuários que estão acessando o sistema usando cada tipo de autenticação.
5. Exiba o cartão **Cluster Security** para exibir os mecanismos de autenticação que estão sendo usados para autenticar usuários em cada cluster.

Se houver alguns usuários acessando o sistema usando um método inseguro ou usando um método que não é recomendado pelo NetApp, você pode desativar o método.

### Exibindo o status de criptografia de todos os volumes

Você pode exibir uma lista de todos os volumes e seu status de criptografia atual para determinar se os dados em seus volumes estão adequadamente protegidos contra o acesso de usuários não autorizados.

#### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Os tipos de criptografia que podem ser aplicados a um volume são:

- Software - volumes protegidos com as soluções de criptografia de software NVE (NetApp volume Encryption) ou NetApp Aggregate Encryption (NAE).
- Hardware - volumes que são protegidos com a criptografia de hardware do NetApp Storage Encryption (NSE).
- Software e hardware - volumes protegidos pela criptografia de software e hardware.
- Nenhum - volumes que não são criptografados.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **Saúde > criptografia volumes**
3. Na exibição **Health: Volumes Encryption**, classifique no campo **Encryption Type** ou use o filtro para exibir volumes que tenham um tipo de criptografia específico ou que não estejam criptografados (Encryption Type of ""None"").

### Visualização do status anti-ransomware de todos os volumes e VMs de storage

Você pode ver uma lista de todos os volumes e VMs de storage (SVMs) e seu status atual anti-ransomware para determinar se os dados nos seus volumes e SVMs estão protegidos adequadamente contra ataques de ransomware.

#### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Para obter mais informações sobre os diferentes status anti-ransomware, "[ONTAP: Ative a anti-ransomware](#)" consulte .

#### Veja os detalhes de segurança de todos os volumes com a detecção antirransomware

##### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **Saúde > Segurança > Anti-ransomware**
3. Na visualização **Segurança: Anti-ransomware**, você pode classificar pelos vários campos ou usar o filtro.



O antirransomware não é compatível com volumes off-line, volumes restritos, volumes SnapLock, volumes FlexGroup, volumes FlexCache, volumes somente SAN, volumes de VMs de storage interrompidas, volumes raiz de VMs de storage ou volumes de proteção de dados.

#### Veja os detalhes de segurança de todas as VMs de storage com a detecção antirransomware

##### Passos

1. No painel de navegação esquerdo, clique em **Storage > Storage VMs**.
2. Selecione **View > Security > Anti-ransomware**. Uma lista de SVMs com o status anti-ransomware é exibida.



O monitoramento anti-ransomware não é compatível com VMs de storage que não têm o protocolo nas ativado.

#### Visualizar todos os eventos de segurança ativos

Você pode exibir todos os eventos de segurança ativos e, em seguida, atribuir cada um deles a um usuário que pode resolver o problema. Além disso, se houver certos eventos de segurança que você não deseja receber, esta lista pode ajudá-lo a identificar os eventos que deseja desativar.

##### Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

##### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.

Por padrão, eventos novos e confirmados são exibidos na página de inventário do Gerenciamento de Eventos.

2. No menu Exibir, selecione **Eventos de segurança ativos**.

A página exibe todos os eventos de Segurança novos e reconhecidos que foram gerados nos últimos 7 dias.

#### Adicionar alertas para eventos de segurança

Você pode configurar alertas para eventos de segurança individuais, como qualquer outro evento recebido pelo Unified Manager. Além disso, se você quiser tratar todos os

eventos de segurança da mesma forma e mandar e-mails para a mesma pessoa, você pode criar um único alerta para notificá-lo quando quaisquer eventos de segurança forem acionados.

#### Antes de começar

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

O exemplo abaixo mostra como criar um alerta para o evento de segurança ""Protocolo Telnet ativado"". Isso enviará um alerta se o acesso Telnet estiver configurado para acesso administrativo remoto ao cluster. Você pode usar essa mesma metodologia para criar alertas para todos os eventos de segurança.

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de alerta**.
2. Na página **Configuração de alerta**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar alerta**, clique em **Nome** e insira um nome e uma descrição para o alerta.
4. Clique em **recursos** e selecione o cluster ou cluster no qual deseja ativar esse alerta.
5. Clique em **Eventos** e execute as seguintes ações:
  - a. Na lista gravidade do evento, selecione **Aviso**.
  - b. Na lista Eventos correspondentes, selecione **Protocolo Telnet ativado**.
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 frequência de notificação, emissão de toques SNMP e execução de um script.
8. Clique em **Salvar**.

#### Desativar eventos de segurança específicos

Todos os eventos são ativados por padrão. Você pode desativar eventos específicos para impedir a geração de notificações para os eventos que não são importantes em seu ambiente. Você pode ativar eventos desativados se quiser retomar o recebimento de notificações para eles.

#### Antes de começar

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

Quando você desativa eventos, os eventos gerados anteriormente no sistema são marcados como obsoletos e os alertas configurados para esses eventos não são acionados. Quando você ativa eventos desativados, as notificações para esses eventos são geradas a partir do próximo ciclo de monitoramento.

#### Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento > Configuração do evento**.
2. Na página Configuração do **evento**, desative ou ative eventos escolhendo uma das seguintes opções:

Se você quiser...	Então faça isso...
Desativar eventos	<ol style="list-style-type: none"> <li>Clique em <b>Desativar</b>.</li> <li>Na caixa de diálogo Desativar eventos, selecione a gravidade <b>Aviso</b>. Esta é a categoria para todos os eventos de segurança.</li> <li>Na coluna Eventos correspondentes, selecione os eventos de segurança que deseja desativar e clique na seta para a direita para mover esses eventos para a coluna Desativar eventos.</li> <li>Clique em <b>Salvar e fechar</b>.</li> <li>Verifique se os eventos desativados são apresentados na vista de lista da página Configuração de eventos.</li> </ol>
Ativar eventos	<ol style="list-style-type: none"> <li>Na lista de eventos desativados, marque a caixa de seleção do evento ou eventos que deseja reativar.</li> <li>Clique em <b>Ativar</b>.</li> </ol>

## Eventos de segurança

Os eventos de segurança fornecem informações sobre o status de segurança de clusters do ONTAP, máquinas virtuais de armazenamento (SVMs) e volumes com base nos parâmetros definidos no *Guia de endurecimento de Segurança do NetApp para ONTAP 9*. Esses eventos notificam você sobre possíveis problemas para que você possa avaliar a gravidade deles e corrigir o problema, se necessário.

Os eventos de segurança são agrupados por tipo de origem e incluem o nome do evento e da armadilha, o nível de impactos e a gravidade. Esses eventos aparecem nas categorias de eventos de VM de armazenamento e cluster.

## Gerenciamento de operações de backup e restauração

Você pode criar backups do Active IQ Unified Manager e usar o recurso de restauração para restaurar o backup para o mesmo sistema (local) ou um novo sistema (remoto) em caso de falha do sistema ou perda de dados.

Há três métodos de backup e restauração dependendo do sistema operacional no qual você instalou o Unified Manager e com base no número de clusters e nós sendo gerenciados:

Sistema operacional	Tamanho da implantação	Método de backup recomendado
VMware vSphere	Qualquer	Snapshot da VMware do dispositivo virtual Unified Manager

Sistema operacional	Tamanho da implantação	Método de backup recomendado
Red Hat Enterprise Linux	Pequeno	Despejo de banco de dados MySQL do Unified Manager
	Grande	Snapshot do NetApp do banco de dados do Unified Manager
Microsoft Windows	Pequeno	Despejo de banco de dados MySQL do Unified Manager
	Grande	NetApp Snapshot do banco de dados do Unified Manager com protocolo iSCSI

Esses diferentes métodos são descritos nas seções a seguir.

### Backup e restauração do Unified Manager em dispositivo virtual

O modelo de backup e restauração do Unified Manager quando instalado em um dispositivo virtual é capturar e restaurar uma imagem do aplicativo virtual completo.

As tarefas a seguir permitem concluir um backup do dispositivo virtual:

1. Desligue a VM e tire um snapshot da VMware do dispositivo virtual Unified Manager.
2. Faça uma cópia Snapshot do NetApp no datastore para capturar o snapshot do VMware.

Se o armazenamento de dados não estiver hospedado em um sistema que executa o software ONTAP, siga as diretrizes do fornecedor de storage para criar um backup do snapshot da VMware.

3. Replique a cópia Snapshot do NetApp, ou equivalente a snapshot, para storage alternativo.
4. Exclua o instantâneo VMware.

Você deve implementar uma programação de backup usando essas tarefas para garantir que o dispositivo virtual do Unified Manager esteja protegido se surgirem problemas.

Para restaurar a VM, você pode usar o snapshot da VMware criado para restaurar a VM para o estado de ponto no tempo de backup.

### Faça backup e restauração usando um despejo de banco de dados MySQL

Um backup de despejo de banco de dados MySQL é uma cópia do banco de dados Active IQ Unified Manager e arquivos de configuração que você pode usar em caso de falha do sistema ou perda de dados. Pode programar uma cópia de segurança para ser escrita num destino local ou num destino remoto. É altamente recomendável que você defina um local remoto externo ao sistema host Active IQ Unified Manager.

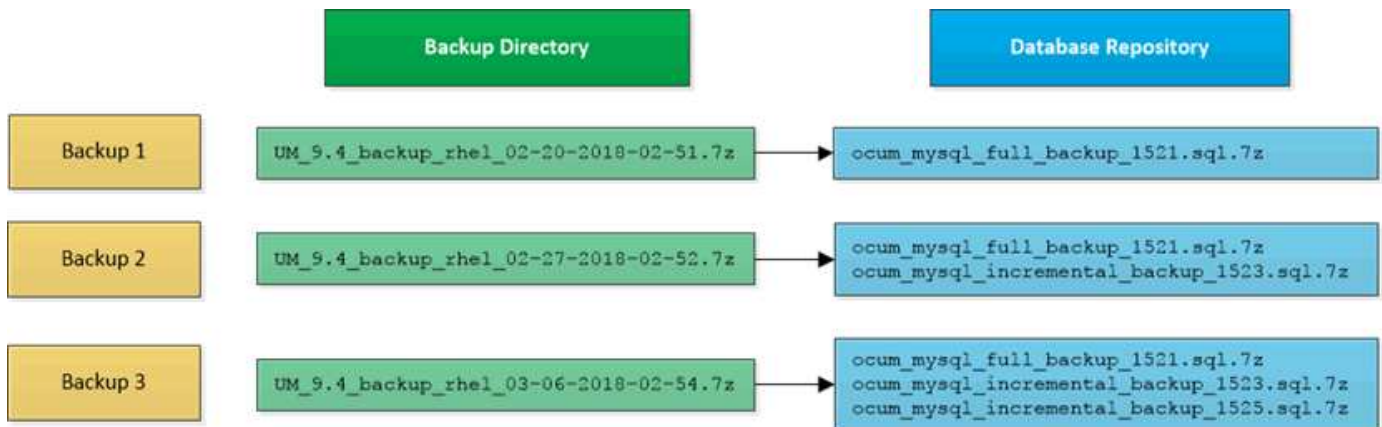




O despejo de banco de dados MySQL é o mecanismo de backup padrão quando o Unified Manager é instalado em um servidor Linux e Windows. No entanto, se o Unified Manager estiver gerenciando um grande número de clusters e nós ou se os backups do MySQL estiverem demorando muitas horas para serem concluídos, você poderá fazer backup usando cópias Snapshot. Esta funcionalidade está disponível no Red Hat Enterprise Linux e Windows.

Um backup de despejo de banco de dados consiste em um único arquivo no diretório de backup e um ou mais arquivos no diretório de repositório de banco de dados. O arquivo no diretório de backup é muito pequeno porque contém apenas um ponteiro para os arquivos localizados no diretório de repositório de banco de dados que são necessários para recriar o backup.

Na primeira vez que você gera um backup de banco de dados, um único arquivo é criado no diretório de backup e um arquivo de backup completo é criado no diretório de repositório de banco de dados. Da próxima vez que você gerar um backup, um único arquivo é criado no diretório de backup e um arquivo de backup incremental é criado no diretório de repositório de banco de dados que contém as diferenças do arquivo de backup completo. Esse processo continua à medida que você cria backups adicionais, até a configuração de retenção máxima, como mostrado na figura a seguir.



Não renomeie ou remova nenhum dos arquivos de backup nesses dois diretórios ou qualquer operação de restauração subsequente falhará.

Se você gravar seus arquivos de backup no sistema local, você deve iniciar um processo para copiar os arquivos de backup para um local remoto para que eles estejam disponíveis caso você tenha um problema de sistema que exija uma restauração completa.

Antes de iniciar uma operação de backup, o Active IQ Unified Manager executa uma verificação de integridade para verificar se todos os arquivos de backup e diretórios de backup necessários existem e são graváveis. Ele também verifica se há espaço suficiente no sistema para criar o arquivo de backup.

### Configurando o destino e o agendamento para backups de despejo de banco de dados

Você pode configurar as configurações de backup de despejo de banco de dados do Unified Manager para definir o caminho de backup do banco de dados, a contagem de retenção e o agendamento de backup. Você pode ativar backups programados diários ou semanais. Por padrão, os backups programados são desativados, mas você deve definir uma programação de backup.

#### Antes de começar

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

- Você deve ter um mínimo de 150 GB de espaço disponível no local que você definir como caminho de backup.

É recomendável usar um local remoto externo ao sistema host do Unified Manager.

- Quando o Unified Manager estiver instalado em um sistema Linux e usando o backup do MySQL, verifique se as permissões e os proprietários a seguir estão definidos no diretório de backup.

Permissões: 0750, propriedade: jboss:maintenance

- Quando o Unified Manager estiver instalado em um sistema Windows e usando o backup MySQL, verifique se somente o administrador tem acesso ao diretório de backup.

Mais tempo é necessário na primeira vez que um backup é executado do que para backups subsequentes, porque o primeiro backup é um backup completo. Um backup completo pode ter mais de 1 GB e pode levar de três a quatro horas. Backups subsequentes são incrementais e exigem menos tempo.



- Se você achar que o número de arquivos de backup incremental é muito grande para o espaço alocado para backups, poderá fazer um backup completo periodicamente para substituir o backup antigo e seus arquivos incrementais. Como outra opção, você pode fazer um backup usando cópias Snapshot.
- O backup realizado durante os 15 dias iniciais de uma nova adição de cluster pode não ser preciso o suficiente para obter os dados históricos de desempenho.

## Passos

1. No painel de navegação à esquerda, clique em **Geral > Backup do banco de dados**.
2. Na página **Backup do banco de dados**, clique em **Backup Settings**.
3. Configure os valores apropriados para um caminho de backup, contagem de retenção e agendamento.

O valor padrão para a contagem de retenção é 10; você pode usar 0 para criar backups ilimitados.

4. Selecione o botão **programado diariamente** ou **programado semanal** e especifique os detalhes da programação.
5. Clique em **aplicar**.

Os arquivos de backup de despejo de banco de dados são criados com base na programação. Você pode ver os arquivos de backup disponíveis na página Backup do banco de dados.

## O que é uma restauração de banco de dados

Uma restauração de banco de dados MySQL é o processo de restauração de um arquivo de backup do Unified Manager existente no mesmo ou em um servidor do Unified Manager diferente. Execute a operação de restauração a partir do console de manutenção do Unified Manager.

Se estiver a executar uma operação de restauro no mesmo sistema (local) e os ficheiros de cópia de segurança estiverem todos armazenados localmente, pode executar a opção de restauro utilizando a localização predefinida. Se você estiver executando uma operação de restauração em um sistema Unified Manager diferente (um sistema remoto), copie o arquivo de backup ou arquivos do armazenamento secundário para o disco local antes de executar a opção de restauração.

Durante o processo de restauração, você será desconectado do Unified Manager. Pode iniciar sessão no

sistema após o processo de restauro estar concluído.

Se você estiver restaurando a imagem de backup para um novo servidor, após a conclusão da operação de restauração, será necessário gerar um novo certificado de segurança HTTPS e reiniciar o servidor do Unified Manager. Você também precisará reconfigurar as configurações de autenticação SAML, se forem necessárias, ao restaurar a imagem de backup para um novo servidor.



Os ficheiros de cópia de segurança antigos não podem ser utilizados para restaurar uma imagem depois de o Unified Manager ter sido atualizado para uma versão mais recente do software. Para economizar espaço, todos os arquivos de backup antigos, exceto o arquivo mais recente, são removidos automaticamente quando você atualiza o Unified Manager.

## Informações relacionadas

["Gerando um certificado de segurança HTTPS"](#)

["Habilitando a autenticação SAML"](#)

["Autenticação com active Directory ou OpenLDAP"](#)

## Restaurar um backup de banco de dados MySQL em um sistema Linux

Se ocorrer perda de dados ou corrupção de dados, você poderá restaurar o Unified Manager para o estado estável anterior com perda mínima de dados. Você pode restaurar o banco de dados do Unified Manager para um sistema Red Hat Enterprise Linux local ou remoto usando o console de manutenção do Unified Manager.

### Antes de começar

- Você deve ter as credenciais de usuário raiz para o host Linux no qual o Unified Manager está instalado.
- Você deve ter uma ID de usuário e senha autorizados para fazer login no console de manutenção do servidor do Unified Manager.
- Você deve ter copiado o arquivo de backup do Unified Manager e o conteúdo do diretório do repositório do banco de dados para o sistema no qual você executará a operação de restauração.

É recomendável que você copie o arquivo de backup para o diretório padrão `/data/ocum-backup`. Os arquivos do repositório de banco de dados devem ser copiados para `/database-dumps-repo`o` subdiretório sob o `/`ocum-backup` diretório.

- Os ficheiros de cópia de segurança têm de ser `.7z` do tipo.

O recurso de restauração é específico da plataforma e específico da versão. Você pode restaurar um backup do Unified Manager somente na mesma versão do Unified Manager. Você pode restaurar um arquivo de backup do Linux ou um arquivo de backup de dispositivo virtual para um sistema Red Hat Enterprise Linux.



Se o nome da pasta de backup contiver um espaço, você deve incluir o caminho absoluto ou caminho relativo em aspas duplas.

## Passos

1. Se você estiver executando uma restauração em um novo servidor, após a instalação do Unified Manager, não inicie a IU nem configure clusters, usuários ou configurações de autenticação quando a instalação for concluída. O arquivo de backup preenche essas informações durante o processo de restauração.

2. Usando o Secure Shell, conete-se ao endereço IP ou ao nome de domínio totalmente qualificado do sistema Unified Manager.
3. Inicie sessão no sistema com o nome e a palavra-passe do utilizador de manutenção (umadmin).
4. Digite o comando `maintenance_console` e pressione Enter.
5. No console de manutenção **Menu Principal**, digite o número da opção **Backup Restore**.
6. Digite o número para o **Restore MySQL Backup**.
7. Quando solicitado, insira o caminho absoluto do arquivo de backup.

```
Bundle to restore from: /data/ocum-  
backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
```

Após a conclusão da operação de restauração, você pode fazer login no Unified Manager.

Depois de restaurar o backup, se o servidor OnCommand Workflow Automation não funcionar, execute as seguintes etapas:

1. No servidor do Workflow Automation, altere o endereço IP do servidor do Unified Manager para apontar para a máquina mais recente.
2. No servidor do Unified Manager, redefina a senha do banco de dados se a aquisição falhar na etapa 1.

#### Restaurar um backup de banco de dados MySQL no Windows

Em caso de perda de dados ou corrupção de dados, você pode usar o recurso de restauração para restaurar o Unified Manager para o estado estável anterior, com perda mínima. Você pode restaurar o banco de dados MySQL do Unified Manager para um sistema Windows local ou um sistema Windows remoto usando o console de manutenção do Unified Manager.

#### Antes de começar

- Você deve ter o Privileges administrador do Windows.
- Você deve ter copiado o arquivo de backup do Unified Manager e o conteúdo do diretório do repositório do banco de dados para o sistema no qual você executará a operação de restauração.

É recomendável que você copie o arquivo de backup para o diretório padrão `\ProgramData\NetApp\OnCommandAppData\ocum\backup`. Os arquivos do repositório de banco de dados devem ser copiados para `\database_dumps_repo` o subdiretório sob o `\backup` diretório.

- Os ficheiros de cópia de segurança têm de ser `.7z` do tipo.

O recurso de restauração é específico da plataforma e específico da versão. Você pode restaurar um backup MySQL do Unified Manager somente na mesma versão do Unified Manager e um backup do Windows pode ser restaurado somente em uma plataforma Windows.



Se os nomes das pastas contiverem um espaço, você deverá incluir o caminho absoluto ou o caminho relativo do arquivo de backup entre aspas duplas.

#### Passos

1. Se você estiver executando uma restauração em um novo servidor, após a instalação do Unified Manager, não inicie a IU nem configure clusters, usuários ou configurações de autenticação quando a instalação for concluída. O arquivo de backup preenche essas informações durante o processo de restauração.
2. Faça login no sistema Unified Manager com credenciais de administrador.
3. Inicie o PowerShell ou prompt de comando como administrador do Windows.
4. Digite o comando `maintenance_console` e pressione Enter.
5. No console de manutenção **Menu Principal**, digite o número da opção **Backup Restore**.
6. Digite o número para o **Restore MySQL Backup**.
7. Quando solicitado, insira o caminho absoluto do arquivo de backup.

```
Bundle to restore from:  
\ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac  
kup_windows_02-20-2020-02-51.7z
```

Após a conclusão da operação de restauração, você pode fazer login no Unified Manager.

Depois de restaurar o backup, se o servidor OnCommand Workflow Automation não funcionar, execute as seguintes etapas:

1. No servidor do Workflow Automation, altere o endereço IP do servidor do Unified Manager para apontar para a máquina mais recente.
2. No servidor do Unified Manager, redefina a senha do banco de dados se a aquisição falhar na etapa 1.

### Faça backup e restauração usando snapshots NetApp

Uma cópia Snapshot do NetApp cria uma imagem pontual do banco de dados e dos arquivos de configuração que você pode usar para restaurar em caso de falha do sistema ou perda de dados. Você agenda periodicamente uma cópia Snapshot para ser gravada em um volume em um dos clusters do ONTAP, para que tenha sempre uma cópia atual.



Essa funcionalidade não está disponível para o Active IQ Unified Manager instalado em um dispositivo virtual.

### Configurando backup no Linux

Se o Active IQ Unified Manager estiver instalado em uma máquina Linux, você poderá decidir configurar o backup e a restauração usando os snapshots do NetApp.

As cópias snapshot demoram muito pouco tempo, geralmente apenas alguns minutos, e o banco de dados do Unified Manager fica bloqueado por um período de tempo muito curto, portanto, há muito pouca interrupção na instalação. A imagem consome espaço de armazenamento mínimo e incorre em sobrecarga de desempenho insignificante, pois registra apenas alterações nos arquivos desde que a última cópia Snapshot foi feita. Como o Snapshot é criado em um cluster do ONTAP, você pode aproveitar outros recursos do NetApp, como o SnapMirror, para criar proteção secundária, se necessário.

Antes de iniciar uma operação de backup, o Unified Manager realiza uma verificação de integridade para

verificar se o sistema de destino está disponível.



- Você pode restaurar uma cópia Snapshot somente na mesma versão do Active IQ Unified Manager.
- Por exemplo, se você criou um backup no Unified Manager 9,16, o backup só poderá ser restaurado em sistemas Unified Manager 9,16.
- Se houver alguma alteração na configuração Snapshot, isso pode fazer com que o snapshot seja inválido.

## Configurando o local de cópia Snapshot

Você pode configurar o volume no qual as cópias Snapshot serão armazenadas em um dos clusters do ONTAP usando o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP.

### Antes de começar

O cluster, a VM de storage e o volume devem atender aos seguintes requisitos:

- Requisitos do cluster:
  - O ONTAP 9.3 ou superior deve ser instalado
  - Ele deve estar geograficamente perto do servidor do Unified Manager
  - Ele pode ser monitorado pelo Unified Manager, mas não é necessário
- Requisitos da VM de storage:
  - A chave de nome e o mapeamento de nomes devem ser definidos para usar "arquivos"
  - Usuários locais criados para corresponder aos usuários do lado do cliente
  - Certifique-se de que todos os acessos de leitura/escrita estão selecionados
  - Certifique-se de que o acesso ao superusuário está definido como "any" na política de exportação
  - NFS para NetApp Snapshot para Linux
  - O NFSv4 deve estar ativado no servidor NFS e no domínio de ID NFSv4 especificado no cliente e na VM de armazenamento
  - O volume deve ser pelo menos o dobro do tamanho do diretório Unified Manager/opt/NetApp/data

Use o comando `du -sh /opt/NetApp/data/` para verificar o tamanho atual.
- Requisitos de volume:
  - O volume deve ser pelo menos o dobro do tamanho do diretório /opt/NetApp/data do Unified Manager
  - O estilo de segurança deve ser definido como UNIX
  - A política de instantâneos locais tem de ser desativada
  - O dimensionamento automático do volume deve estar ativado
  - O nível de serviço de desempenho deve ser definido para uma política com IOPS alto e baixa latência, como o "Extreme"

Para obter as etapas detalhadas para criar o volume NFS, consulte ["Como configurar o NFSv4 no ONTAP 9"](#) e o ["Guia expresso de configuração de NFS do ONTAP 9"](#).

## Especificando o local de destino para cópias Snapshot

Você deve configurar o local de destino para cópias Snapshot do Active IQ Unified Manager em um volume que já tenha configurado em um de seus clusters do ONTAP. Você deve usar o console de manutenção para definir a localização.

- Você deve ter as credenciais de usuário raiz para o host Linux no qual o Active IQ Unified Manager está instalado.
- Você deve ter uma ID de usuário e senha autorizados para fazer login no console de manutenção do servidor do Unified Manager.
- Você deve ter o endereço IP de gerenciamento de cluster, o nome da VM de armazenamento, o nome do volume e o nome de usuário e senha do sistema de armazenamento.
- Você deve ter montado o volume no host Active IQ Unified Manager e deve ter o caminho de montagem.

### Passos

1. Use Shell seguro para se conectar ao endereço IP ou FQDN do sistema Active IQ Unified Manager.
2. Inicie sessão no sistema com o nome e a palavra-passe do utilizador de manutenção (umadmin).
3. Digite o comando `maintenance_console` e pressione Enter.
4. No console de manutenção **Menu Principal**, digite o número da opção **Backup Restore**.
5. Digite o número para **Configurar cópia de segurança de instantâneo do NetApp**.
6. Introduza o número para configurar o NFS.
7. Revise as informações que você precisará fornecer e insira o número de **Digite os detalhes da configuração de backup**.
8. Para identificar o volume em que o instantâneo será gravado, insira o endereço IP da interface de gerenciamento de cluster, o nome da VM de armazenamento, o nome do volume, o nome do LUN, o nome do usuário e a senha do sistema de armazenamento e o caminho de montagem.
9. Verifique essas informações e `y` digite `.`

O sistema executa as seguintes tarefas:

- Estabelece a conexão com o cluster
  - Pára todos os serviços
  - Cria um novo diretório no volume e copia os arquivos de configuração do banco de dados Active IQ Unified Manager
  - Exclui os arquivos do Active IQ Unified Manager e cria um link simbólico para o novo diretório de banco de dados
  - Reinicia todos os serviços
10. Saia do console de manutenção e inicie a interface do Active IQ Unified Manager para criar um agendamento para a cópia Snapshot se você ainda não tiver feito isso.

### Configurando backup no Windows

O Active IQ Unified Manager suporta backup e restauração usando snapshots NetApp no sistema operacional Windows com a ajuda de LUN usando protocolo iSCSI.

O backup baseado em snapshot pode ser feito enquanto todos os serviços do Unified Manager estão em

execução. Um estado consistente do banco de dados é capturado como parte do Snapshot, pois o backup coloca um bloqueio de leitura global em todo o banco de dados, o que impede qualquer gravação simultânea. Para que o sistema Unified Manager instalado no sistema operacional Windows execute backup e restauração usando snapshots do NetApp, primeiro você deve configurar o backup do Unified Manager para Snapshot com base no console de manutenção.

Antes de configurar o Unified Manager para a criação de cópias Snapshot, execute as seguintes tarefas de configuração.

- Configurar cluster ONTAP
- Configurar a máquina host do Windows

### **Configurando o local de backup para Windows**

Você deve configurar o volume para armazenar cópias Snapshot após fazer backup do Unified Manager no Windows.

#### **Antes de começar**

O cluster, a VM de storage e o volume devem atender aos seguintes requisitos:

- Requisitos do cluster:
  - O ONTAP 9.3 ou superior deve ser instalado
  - Ele deve estar geograficamente perto do servidor do Unified Manager
  - Ele é monitorado pelo Unified Manager
- Requisitos da VM de storage:
  - Conetividade iSCSI no cluster ONTAP
  - O protocolo iSCSI deve estar ativado para a máquina configurada
  - Você deve ter um volume dedicado e LUN para configuração de backup. O volume selecionado deve conter apenas um LUN e nada mais.
  - O tamanho do LUN deve ser pelo menos o dobro do tamanho de dados esperado para ser Tratado no 9,9 Active IQ Unified Manager.  
  
Isso também define o mesmo requisito de tamanho no volume.
  - Certifique-se de que todos os acessos de leitura/escrita estão selecionados
  - Certifique-se de que o acesso ao superusuário está definido como "any" na política de exportação
- Requisitos de volume e LUN:
  - O volume deve ser pelo menos o dobro do tamanho do diretório de dados MySQL do Unified Manager.
  - O estilo de segurança deve ser definido para Windows
  - A política de instantâneos locais tem de ser desativada
  - O dimensionamento automático do volume deve estar ativado
  - O nível de serviço de desempenho deve ser definido para uma política com IOPS alto e baixa latência, como o "Extreme"



## Configurando o cluster ONTAP

Você precisa executar algumas etapas de pré-configuração nos clusters do ONTAP antes de fazer backup e restaurar o Active IQ Unified Manager usando a cópia Snapshot em sistemas Windows.

Você pode configurar o cluster do ONTAP usando o prompt de comando ou a interface do usuário do Gerenciador do sistema. A configuração do cluster ONTAP envolve a configuração de LIFs de dados para estarem disponíveis para serem atribuídos como LIFs iSCSI à VM de armazenamento. A próxima etapa é configurar uma VM de armazenamento habilitada para iSCSI usando a interface do usuário do System Manager. Você precisará configurar uma rota de rede estática para essa VM de armazenamento para controlar como os LIFs usam a rede para o tráfego de saída.



Você deve ter um volume dedicado e um LUN para configuração de backup. O volume selecionado deve incluir apenas um LUN. O tamanho do LUN deve ser pelo menos o dobro do tamanho de dados esperado para ser Tratado pelo Active IQ Unified Manager.

Você precisa executar a seguinte configuração:

### Passos

1. Configure uma VM de armazenamento habilitada para iSCSI ou use uma VM de armazenamento existente que tenha a mesma configuração.
2. Configure uma rota de rede para a VM de armazenamento configurada.
3. Configure um volume de capacidade adequada e um único LUN no interior, garantindo que o volume seja dedicado apenas a este LUN.



Em um cenário em que o LUN é criado no System Manager, o desmapeamento do LUN pode excluir o grupo e a restauração pode falhar. Para evitar esse cenário, certifique-se de que, ao criar um LUN, ele seja criado explicitamente e não seja excluído quando o LUN não for mapeado.

4. Configure um grupo de iniciadores na VM de armazenamento.
5. Configurar um conjunto de portas.
6. Integre o igrop com o portset.
7. Mapeie o LUN para o grupo.

## Configurando a máquina host do Windows

Você precisa configurar sua máquina host do Windows antes de poder usar a captura Instantânea do NetApp para fazer backup e restaurar o Active IQ Unified Manager. Para iniciar o iniciador iSCSI da Microsoft em uma máquina host do Windows, digite "iscsi" na barra de pesquisa e clique em **Iniciador iSCSI**.

### Antes de começar

Você deve limpar todas as configurações anteriores na máquina host.

Se você estiver tentando iniciar o iniciador iSCSI em uma nova instalação do Windows, será solicitado a confirmação e, na confirmação, a caixa de diálogo Propriedades iSCSI será exibida. Se for uma instalação do Windows existente, a caixa de diálogo Propriedades iSCSI será exibida com um destino inativo ou tentando se

conetar. Portanto, você precisará garantir que todas as configurações anteriores no host do Windows sejam removidas.

### Passos

1. Limpe todas as configurações anteriores na máquina host.
2. Descubra o portal de destino.
3. Conecte-se ao portal de destino.
4. Conecte-se usando multipath ao portal de destino.
5. Descubra os dois LIFs.
6. Descubra o LUN configurado na máquina Windows como um dispositivo.
7. Configure o LUN descoberto como uma nova unidade de volume no Windows.

### Especificando o local de destino para cópias Snapshot no Windows

Você deve configurar o local de destino para cópias Snapshot do Active IQ Unified Manager em um volume que já tenha configurado em um de seus clusters do ONTAP. Você deve usar o console de manutenção para definir a localização.

- Você deve ter o privilégio de administrador para o host Windows no qual o Active IQ Unified Manager está instalado.
- Você deve ter uma ID de usuário e senha autorizados para fazer login no console de manutenção do servidor do Unified Manager.
- Você deve ter o endereço IP de gerenciamento de cluster, o nome da VM de armazenamento, o nome do volume, o nome do LUN e o nome de usuário e a senha do sistema de armazenamento.
- Você deve ter montado o volume como uma unidade de rede para o host Active IQ Unified Manager e deve ter a unidade de montagem.

### Passos

1. Usando o Power Shell, conecte-se ao endereço IP ou ao nome de domínio totalmente qualificado do sistema Active IQ Unified Manager.
2. Inicie sessão no sistema com o nome e a palavra-passe do utilizador de manutenção (umadmin).
3. Digite o comando `maintenance_console` e pressione Enter.
4. No console de manutenção **Menu Principal**, digite o número da opção **Backup Restore**.
5. Digite o número para **Configurar cópia de segurança de instantâneo do NetApp**.
6. Introduza o número para configurar iSCSI.
7. Revise as informações que você precisará fornecer e insira o número de **Digite os detalhes da configuração de backup**.
8. Para identificar o volume em que o instantâneo será gravado, insira o endereço IP da interface de gerenciamento de cluster, o nome da VM de armazenamento, o nome do volume, o nome do LUN, o nome do usuário e a senha do sistema de armazenamento e a unidade de montagem.
9. Verifique essas informações e `y` digite .

O sistema executa as seguintes tarefas:

- A VM de storage é validada

- O volume está validado
  - A unidade de montagem e o estado estão validados
  - Existência e estado do LUN
  - Existência de unidade de rede
  - A existência de espaço recomendado (mais de duas vezes do diretório de dados mysql) no volume montado é validada
  - Caminho LUN correspondente ao LUN dedicado no volume
  - nome do grupo
  - GUID do volume onde a unidade de rede está montada
  - Iniciador iSCSI usado para se comunicar com o ONTAP
10. Saia do console de manutenção e inicie a interface do Active IQ Unified Manager para criar um agendamento para cópias Snapshot.

### Configurando o backup por cópia Snapshot do console de manutenção

Para fazer o backup do Active IQ Unified Manager usando a cópia Snapshot, você deve executar algumas etapas de configuração no console de manutenção.

#### Antes de começar

Você deve ter os seguintes detalhes para o seu sistema:

- Endereço IP do cluster
- Nome da VM de storage
- Nome do volume
- Nome LUN
- Caminho de montagem
- Credenciais do sistema de storage

#### Passos

1. Acesse o console de manutenção do Unified Manager.
2. Digite 4 para selecionar **Backup Restore**.
3. Digite 2 para selecionar **Backup e restauração usando Instantâneo do NetApp**.



Se você quiser alterar a configuração de backup, digite 3 para selecionar **Atualizar Configuração de backup instantâneo do NetApp**. Só pode atualizar a palavra-passe.

4. No menu, digite 1 para selecionar **Configurar cópia de segurança de instantâneo do NetApp**.
5. Introduza 1 para fornecer as informações necessárias.
6. Forneça o nome de usuário e a senha para o console de manutenção e forneça a confirmação de que o LUN está montado no host.

Em seguida, o processo verifica se o diretório de dados, o caminho LUN, a VM de armazenamento, os volumes, a disponibilidade de espaço, a unidade e assim por diante fornecidos por você estão corretos. As operações que prosseguem em segundo plano são:

- Os serviços são interrompidos
- O diretório do banco de dados é movido para o armazenamento montado
- O diretório do banco de dados é excluído e os links simbólicos são estabelecidos
- Os serviços são reiniciados após a conclusão da configuração na interface do Active IQ Unified Manager, o tipo de backup é modificado para captura Instantânea do NetApp e reflete na interface do usuário como backup do banco de dados (baseado em captura Instantânea).

Antes de iniciar uma operação de backup, você deve verificar se há alguma alteração na configuração Snapshot porque pode fazer com que o snapshot seja inválido. Suponha que você configurou o backup na unidade G e o Snapshot obtido. Posteriormente, você reconfigurou o backup para a unidade E e os dados são salvos na unidade E e de acordo com a nova configuração. Se você tentar restaurar o Snapshot tomado enquanto ele estava na unidade G, ele falhará com o erro de que a unidade G não existe.

#### Definir uma agenda de backup para Linux e Windows

Você pode configurar a programação em que as cópias Snapshot do Unified Manager são criadas usando a IU do Unified Manager.

#### Antes de começar

- Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado as configurações para criar cópias Snapshot a partir do console de manutenção para identificar o destino onde os snapshots serão criados.

As cópias snapshot são criadas em apenas alguns minutos, e o banco de dados do Unified Manager fica bloqueado apenas por alguns segundos.



O backup realizado durante os 15 dias iniciais de uma nova adição de cluster pode não ser preciso o suficiente para obter os dados históricos de desempenho.

#### Passos

1. No painel de navegação à esquerda, clique em **Geral > Backup do banco de dados**.
2. Na página **Backup do banco de dados**, clique em **Backup Settings**.
3. Introduza o número máximo de cópias Snapshot que pretende manter no campo **contagem de retenção**.

O valor padrão para a contagem de retenção é 10. O número máximo de cópias Snapshot é determinado pela versão do software ONTAP no cluster. Você pode deixar este campo em branco para implementar o valor máximo independentemente da versão do ONTAP.

4. Selecione o botão **programado diariamente** ou **programado semanal** e especifique os detalhes da programação.
5. Clique em **aplicar**.

As cópias snapshot são criadas com base na programação. Você pode ver os arquivos de backup disponíveis na página Backup do banco de dados.

Devido à importância desse volume e dos instantâneos, você pode querer criar um ou dois alertas para esse volume para que você seja notificado quando:

- O espaço de volume está 90% cheio. Use o evento **espaço de volume cheio** para configurar o alerta.

Você pode adicionar capacidade ao volume usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP para que o banco de dados do Unified Manager não fique sem espaço.

- O número de instantâneos está próximo de atingir o número máximo. Use o evento  **muitas cópias Snapshot** para configurar o alerta.

Você pode excluir snapshots mais antigos usando o Gerenciador de sistemas do ONTAP ou a CLI do ONTAP para que sempre haja espaço para novas cópias Snapshot.

Configure alertas na página Configuração de alertas.

### Restaurar o Unified Manager usando cópias Snapshot

Se ocorrer perda de dados ou corrupção de dados, você poderá restaurar o Unified Manager para o estado estável anterior com perda mínima de dados. Você pode restaurar o banco de dados Snapshot do Unified Manager para um sistema operacional local ou remoto usando o console de manutenção do Unified Manager.

#### Antes de começar

- Você deve ter as credenciais de usuário raiz para o host Linux e o Privileges administrativo para a máquina host Windows na qual o Unified Manager está instalado.
- Você deve ter uma ID de usuário e senha autorizados para fazer login no console de manutenção do servidor do Unified Manager.

O recurso de restauração é específico da plataforma e específico da versão. Você pode restaurar um backup do Unified Manager somente na mesma versão do Unified Manager.

#### Passos

1. Conecte-se ao endereço IP ou ao nome de domínio totalmente qualificado do sistema Unified Manager.
  - Linux: Shell seguro
  - Windows: Power Shell
2. Faça login no sistema com as credenciais do usuário raiz.
3. Digite o comando `maintenance_console` e pressione Enter.
4. No console de manutenção **Menu Principal**, digite 4 para a opção **Backup Restore**.
5. Digite 2 para selecionar **Backup e Restauração usando Instantâneo do NetApp**.

Se você estiver executando uma restauração em um novo servidor, após a instalação do Unified Manager, não inicie a IU nem configure clusters, usuários ou configurações de autenticação quando a instalação for concluída. Digite 1 para selecionar **Configurar backup instantâneo do NetApp** e configure as configurações para cópias snapshot como estão no sistema original.

6. Digite 3 para selecionar **Restaurar usando Instantâneo do NetApp**.
7. Selecione a cópia Snapshot a partir da qual você deseja restaurar o Unified Manager. Pressione **Enter**.
8. Depois que o processo de restauração for concluído, faça login na interface de usuário do Unified Manager.

Depois de restaurar o backup, se o servidor do Workflow Automation não funcionar, execute as seguintes etapas:

1. No servidor do Workflow Automation, altere o endereço IP do servidor do Unified Manager para apontar para a máquina mais recente.
2. No servidor do Unified Manager, redefina a senha do banco de dados se a aquisição falhar na etapa 1.

### Modificar o tipo de cópia de segurança

Se você quiser alterar o tipo de backup do sistema Active IQ Unified Manager, use as opções do console de manutenção. A opção **Unconfigure NetApp Snapshot Backup** permite que você volte para o backup baseado em MySQL.

#### Antes de começar

Você deve ter uma ID de usuário e senha autorizados para fazer login no console de manutenção do servidor do Unified Manager.

#### Passos

1. Acesse à consola de manutenção.
2. Selecione 4 no **Menu Principal** para fazer backup e restauração.
3. Selecione 2 no **Backup and Restore Menu**.
4. Selecione 4 para **Unconfigure o backup instantâneo do NetApp**.

As ações que são executadas são exibidas, que são, parar os serviços, quebrar o link simbólico, mover os dados do armazenamento para o diretório e, em seguida, iniciar os serviços novamente.

Depois que o método de backup é modificado, o mecanismo de backup é alterado de cópia Snapshot para backup MySQL padrão. Esta alteração é apresentada na seção cópia de segurança da base de dados das definições gerais.

### Backup sob demanda para Unified Manager

Você pode usar a interface de usuário do Active IQ Unified Manager para gerar backup sob demanda sempre que necessário. O backup sob demanda permite que você crie instantaneamente um backup usando o método de backup existente. O backup sob demanda não diferencia entre o MySQL ou o backup baseado no NetApp Snapshot.

Você pode executar o backup sob demanda usando o botão **Backup Now** na página Backup do banco de dados. O backup sob demanda não depende das programações que você configurou para o Active IQ Unified Manager.

### Migração de um dispositivo virtual do Unified Manager para um sistema Linux

Você pode restaurar um backup de despejo de banco de dados MySQL do Unified Manager de um dispositivo virtual para um sistema Red Hat Enterprise Linux se quiser alterar o sistema operacional do host no qual o Unified Manager está sendo executado.

#### Antes de começar

- No dispositivo virtual:
  - Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.
  - Você deve saber o nome do usuário de manutenção do Unified Manager para a operação de

restauração.

- No sistema Linux:
  - Você deve ter instalado o Unified Manager em um servidor Linux seguindo as instruções no ["Instalar o Unified Manager em sistemas Linux"](#).
  - A versão do Unified Manager neste servidor deve ser a mesma do dispositivo virtual a partir do qual você está usando o arquivo de backup.
  - Não inicie a IU nem configure clusters, usuários ou configurações de autenticação no sistema Linux após a instalação. O arquivo de backup preenche essas informações durante o processo de restauração.
  - Você deve ter as credenciais de usuário raiz para o host Linux.

Estas etapas descrevem como criar um arquivo de backup no dispositivo virtual, copiar os arquivos de backup para o Red Hat Enterprise Linux e restaurar o backup do banco de dados para o novo sistema.

### Passos

1. No dispositivo virtual, clique em **Management > Database Backup**.
2. Na página **Backup do banco de dados**, clique em **Backup Settings**.
3. Altere o caminho de backup para `/jail/support`.
4. Na seção Agendamento, selecione **programado diariamente** e insira um tempo depois da hora atual para que o backup seja criado em breve.
5. Clique em **aplicar**.
6. Aguarde algumas horas para que o backup seja gerado.

Um backup completo pode ter mais de 1 GB e pode levar de três a quatro horas para ser concluído.

7. Faça login como o usuário raiz no host Linux no qual o Unified Manager está instalado e copie os arquivos de backup de `/support` no dispositivo virtual usando SCP.

```
root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .
```

```
root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
```

Certifique-se de ter copiado o arquivo de backup `.7z` e todos os arquivos de repositório `.7z` no subdiretório `/database-dumps-repo`.

8. No prompt de comando, restaure o backup: `um backup restore -f /<backup_file_path>/<backup_file_name>`

```
um backup restore -f /UM_9.7.N151113.1348_backup_unix_02-12-2019-04-16.7z
```

9. Após a conclusão da operação de restauração, faça login na IU da Web do Unified Manager.

Você deve executar as seguintes tarefas:

- Gere um novo certificado de segurança HTTPS e reinicie o servidor do Unified Manager.
- Altere o caminho de backup para a configuração padrão do seu sistema Linux (`/data/ocum-backup`), ou para um novo caminho de sua escolha, porque não há nenhum caminho `/jail/support` no sistema Linux.
- Reconfigure ambos os lados da conexão do Workflow Automation, se o WFA estiver sendo usado.
- Reconfigure as configurações de autenticação SAML, se você estiver usando SAML.

Depois de verificar se tudo está sendo executado como esperado no sistema Linux, você pode desligar e remover o dispositivo virtual do Unified Manager.

## Gerenciamento de scripts

Você pode usar scripts para modificar ou atualizar automaticamente vários objetos de armazenamento no Unified Manager. O script está associado a um alerta. Quando um evento aciona um alerta, o script é executado. Você pode carregar scripts personalizados e testar sua execução quando um alerta é gerado.

A capacidade de carregar scripts para o Unified Manager e executá-los é ativada por padrão. Se a sua organização não quiser permitir esta funcionalidade por motivos de segurança, pode desativar esta funcionalidade a partir de **Gestão de armazenamento > Definições de funcionalidade**.

### Como os scripts funcionam com alertas

Você pode associar um alerta ao script para que o script seja executado quando um alerta for gerado para um evento no Unified Manager. Você pode usar os scripts para resolver problemas com objetos de armazenamento ou identificar quais objetos de armazenamento estão gerando os eventos.

Quando um alerta é gerado para um evento no Unified Manager, um e-mail de alerta é enviado aos destinatários especificados. Se você associou um alerta a um script, o script será executado. Você pode obter os detalhes dos argumentos passados para o script a partir do e-mail de alerta.



Se você criou um script personalizado e o associou a um alerta para um tipo de evento específico, as ações serão realizadas com base no script personalizado para esse tipo de evento e as ações **Fix it** não estarão disponíveis por padrão na página ações de gerenciamento ou no painel do Unified Manager.

O script usa os seguintes argumentos para execução:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Você pode usar os argumentos em seus scripts e coletar informações de eventos relacionados ou modificar objetos de armazenamento.

### Exemplo para obter argumentos de scripts



```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

Quando um alerta é gerado, este script é executado e a seguinte saída é exibida:

```
-eventID : 290
-eventSourceID : 4138
```

### Adicionando scripts

Você pode adicionar scripts no Unified Manager e associar os scripts a alertas. Esses scripts são executados automaticamente quando um alerta é gerado e permitem obter informações sobre objetos de armazenamento para os quais o evento é gerado.

#### Antes de começar

- Você deve ter criado e salvo os scripts que deseja adicionar ao servidor do Unified Manager.
- Os formatos de arquivo suportados para scripts são Perl, Shell, PowerShell, Python e .bat arquivos.

Plataforma na qual o Unified Manager está instalado	Idiomas suportados
VMware	Scripts Perl e Shell
Linux	Scripts Perl, Python e Shell
Windows	Scripts PowerShell, Perl, Python e .bat

- Para scripts Perl, Perl deve ser instalado no servidor Unified Manager. Para instalações VMware, o Perl 5 é instalado por padrão e os scripts suportam apenas o que o Perl 5 suporta. Se o Perl foi instalado após o Unified Manager, você deve reiniciar o servidor do Unified Manager.
- Para scripts do PowerShell, a política de execução apropriada do PowerShell deve ser definida no servidor Windows para que os scripts possam ser executados.



Se o script criar arquivos de log para acompanhar o andamento do script de alerta, você deve garantir que os arquivos de log não sejam criados em qualquer lugar na pasta de instalação do Unified Manager.

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

Você pode fazer upload de scripts personalizados e reunir detalhes do evento sobre o alerta.



Se você não vir esse recurso disponível na interface do usuário, é porque a funcionalidade foi desativada pelo administrador. Se necessário, pode ativar esta funcionalidade a partir de **Gestão de armazenamento > Definições de funcionalidade**.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Scripts**.
2. Na página **Scripts**, clique em **Add**.
3. Na caixa de diálogo **Add Script**, clique em **Browse** para selecionar seu arquivo de script.
4. Insira uma descrição para o script selecionado.
5. Clique em **Add**.

### Eliminar scripts

Você pode excluir um script do Unified Manager quando o script não for mais necessário ou válido.

#### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- O script não deve estar associado a um alerta.

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Scripts**.
2. Na página **Scripts**, selecione o script que deseja excluir e clique em **Delete**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

### Testando a execução de script

Você pode verificar se o script é executado corretamente quando um alerta é gerado para um objeto de armazenamento.

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter carregado um script no formato de arquivo suportado para o Unified Manager.

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Scripts**.
2. Na página **Scripts**, adicione seu script de teste.
3. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de alerta**.
4. Na página **Configuração de alerta**, execute uma das seguintes ações:

Para...	Faça isso...
Adicione um alerta	<ol style="list-style-type: none"> <li>a. Clique em <b>Add</b>.</li> <li>b. Na seção ações, associe o alerta ao script de teste.</li> </ol>
Edite um alerta	<ol style="list-style-type: none"> <li>a. Selecione um alerta e clique em <b>Editar</b>.</li> <li>b. Na seção ações, associe o alerta ao script de teste.</li> </ol>

5. Clique em **Salvar**.
6. Na página **Configuração de alerta**, selecione o alerta que você adicionou ou modificou e clique em **Teste**.

O script é executado com o argumento "-teSt", e um alerta de notificação é enviado para os endereços de e-mail que foram especificados quando o alerta foi criado.

## Gerenciamento e monitoramento de grupos

É possível criar grupos no Unified Manager para gerenciar objetos de storage.

### Compreender grupos

É possível criar grupos no Unified Manager para gerenciar objetos de storage. Entender os conceitos sobre grupos e como as regras de grupo permitem adicionar objetos de armazenamento a um grupo ajudará você a gerenciar os objetos de armazenamento em seu ambiente.

#### O que é um grupo

Um grupo é uma coleção dinâmica de objetos de storage heterogêneos (clusters, SVMs ou volumes). É possível criar grupos no Unified Manager para gerenciar facilmente um conjunto de objetos de storage. Os membros de um grupo podem mudar, dependendo dos objetos de storage que são monitorados pelo Unified Manager em um momento.

- Cada grupo tem um nome único.
- Você deve configurar um mínimo de uma regra de grupo para cada grupo.
- Você pode associar um grupo a mais de uma regra de grupo.
- Cada grupo pode incluir vários tipos de objetos de storage, como clusters, SVMs ou volumes.
- Os objetos de storage são adicionados dinamicamente a um grupo com base no momento em que uma regra de grupo é criada ou quando o Unified Manager conclui um ciclo de monitoramento.
- Você pode aplicar simultaneamente ações a todos os objetos de storage em um grupo, como definir limites para volumes.

#### Como as regras de grupo funcionam para grupos

Uma regra de grupo é um critério que você define para permitir que objetos de armazenamento (volumes, clusters ou SVMs) sejam incluídos em um grupo específico. Você pode usar grupos de condições ou condições para definir a regra de grupo para um grupo.

- Você deve associar uma regra de grupo a um grupo.
- Você deve associar um tipo de objeto para uma regra de grupo; somente um tipo de objeto está associado a uma regra de grupo.
- Objetos de armazenamento são adicionados ou removidos do grupo após cada ciclo de monitoramento ou quando uma regra é criada, editada ou excluída.
- Uma regra de grupo pode ter um ou mais grupos de condição e cada grupo de condição pode ter uma ou mais condições.

- Os objetos de armazenamento podem pertencer a vários grupos com base nas regras de grupo criadas.

## Condições

Você pode criar vários grupos de condições e cada grupo de condições pode ter uma ou mais condições. Você pode aplicar todos os grupos de condição definidos em uma regra de grupo para grupos, a fim de especificar quais objetos de armazenamento estão incluídos no grupo.

As condições dentro de um grupo de condições são executadas usando LÓGICA e. Todas as condições de um grupo de condições devem ser atendidas. Quando você cria ou modifica uma regra de grupo, uma condição é criada que aplica, seleciona e agrupa apenas os objetos de armazenamento que satisfazem todas as condições no grupo condição. Você pode usar várias condições em um grupo de condições quando quiser restringir o escopo de quais objetos de armazenamento incluir em um grupo.

Você pode criar condições com objetos de armazenamento usando os seguintes operandos e operador e especificando o valor necessário.

Tipo de objeto de storage	Operandos aplicáveis
Volume	<ul style="list-style-type: none"> <li>• Nome do objeto</li> <li>• Nome do cluster proprietário</li> <li>• Possuir nome SVM</li> <li>• Anotações</li> </ul>
SVM	<ul style="list-style-type: none"> <li>• Nome do objeto</li> <li>• Nome do cluster proprietário</li> <li>• Anotações</li> </ul>
Cluster	<ul style="list-style-type: none"> <li>• Nome do objeto</li> <li>• Anotações</li> </ul>

Quando você seleciona a anotação como um operando para qualquer objeto de armazenamento, o operador "is" está disponível. Para todos os outros operandos, você pode selecionar "is" ou "contains" como operador.

- Operando

A lista de operandos no Unified Manager muda com base no tipo de objeto selecionado. A lista inclui o nome do objeto, o nome do cluster proprietário, o nome do SVM e as anotações definidas no Unified Manager.

- Operador

A lista de operadores muda com base no operando selecionado para uma condição. Os operadores suportados no Unified Manager são "is" e "contém".

Quando você seleciona o operador "'is'", a condição é avaliada para correspondência exata do valor do operando com o valor fornecido para o operando selecionado.

Quando você seleciona o operador "'contém'", a condição é avaliada para atender a um dos seguintes critérios:

- O valor do operando é uma correspondência exata com o valor fornecido para o operando selecionado
- O valor do operando contém o valor fornecido para o operando selecionado
- Valor

O campo valor muda com base no operand selecionado.

### Exemplo de uma regra de grupo com condições

Considere um grupo de condições para um volume com as duas seguintes condições:

- O nome contém "vol"
- O nome da SVM é "dATA\_svm"

Esse grupo de condição seleciona todos os volumes que incluem "vol" em seus nomes e que são hospedados em SVMs com o nome "dATA\_svm".

### Grupos de condições

Os grupos de condição são executados usando OU lógico e, em seguida, aplicados a objetos de armazenamento. Os objetos de armazenamento devem satisfazer um dos grupos de condições a serem incluídos em um grupo. Os objetos de armazenamento de todos os grupos de condições são combinados. Você pode usar grupos de condições para aumentar o escopo dos objetos de armazenamento a serem incluídos em um grupo.

### Exemplo de uma regra de grupo com grupos de condição

Considere dois grupos de condições para um volume, com cada grupo contendo as seguintes duas condições:

- Grupo de condições 1
  - O nome contém "vol"
  - O nome do SVM é "dATA\_svm" grupo de condições 1 seleciona todos os volumes que incluem "vol" em seus nomes e que são hospedados em svms com o nome "dATA\_svm".
- Grupo de condições 2
  - O nome contém "vol"
  - O valor de anotação da prioridade de dados é o grupo de condições "crítico" 2 seleciona todos os volumes que incluem "vol" em seus nomes e que são anotados com o valor de anotação de prioridade de dados como "crítico".

Quando uma regra de grupo contendo esses dois grupos de condições é aplicada em objetos de armazenamento, os seguintes objetos de armazenamento são adicionados a um grupo selecionado:

- Todos os volumes que incluem "vol" em seus nomes e que são hospedados no SVM com o nome "dATA\_svm".
- Todos os volumes que incluem "vol" em seus nomes e que são anotados com o valor de anotação de prioridade de dados "crítico".

### Como as ações de grupo funcionam em objetos de armazenamento

Uma ação de grupo é uma operação que é executada em todos os objetos de

armazenamento em um grupo. Por exemplo, você pode configurar a ação de grupo de limite de volume para alterar simultaneamente os valores de limite de volume de todos os volumes em um grupo.

Os grupos suportam tipos de ação de grupo exclusivos. Você pode ter um grupo com apenas um tipo de ação de grupo de limite de integridade de volume. No entanto, você pode configurar um tipo diferente de ação de grupo, se disponível, para o mesmo grupo. A classificação de uma ação de grupo determina a ordem em que a ação é aplicada aos objetos de armazenamento. A página de detalhes de um objeto de armazenamento fornece informações sobre qual ação de grupo é aplicada no objeto de armazenamento.

### Exemplo de ações de grupo únicas

Considere um volume A que pertence aos grupos G1 e G2 e as seguintes ações de grupo de limite de integridade do volume estão configuradas para esses grupos:

- `Change_capacity_threshold` ação de grupo com classificação 1, para configurar a capacidade do volume
- `Change_snapshot_copies` Ação de grupo com classificação 2, para configurar as cópias Snapshot do volume

A `Change_capacity_threshold` ação de grupo sempre tem prioridade sobre a `Change_snapshot_copies` ação de grupo e é aplicada ao volume A. quando o Unified Manager conclui um ciclo de monitoramento, os eventos relacionados ao limite de integridade do volume A são reavaliados de acordo com a `Change_capacity_threshold` ação do grupo. Não é possível configurar outro tipo de limite de volume de ação de grupo para o grupo G1 ou G2.

### Adicionando grupos

É possível criar grupos para combinar clusters, volumes e máquinas virtuais de storage (SVMs) para facilitar o gerenciamento.

#### Antes de começar

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

Você pode definir regras de grupo para adicionar ou remover membros do grupo e modificar ações de grupo para o grupo.

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **Groups**, clique em **Add**.
3. Na caixa de diálogo **Adicionar grupo**, insira um nome e uma descrição para o grupo.
4. Clique em **Add**.

### Editar grupos

Você pode editar o nome e a descrição de um grupo criado no Unified Manager.

#### Antes de começar

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

Quando você edita um grupo para atualizar o nome, você deve especificar um nome exclusivo; você não pode

usar um nome de grupo existente.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **Groups**, selecione o grupo que deseja editar e clique em **Edit**.
3. Na caixa de diálogo **Editar grupo**, altere o nome, a descrição ou ambos para o grupo.
4. Clique em **Salvar**.

### Eliminar grupos

Você pode excluir um grupo do Unified Manager quando o grupo não for mais necessário.

#### Antes de começar

- Nenhum dos objetos de storage (clusters, SVMs ou volumes) deve estar associado a qualquer regra de grupo associada ao grupo que você deseja excluir.
- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **Groups**, selecione o grupo que deseja excluir e clique em **Delete**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

A exclusão de um grupo não exclui as ações de grupo associadas ao grupo. No entanto, essas ações de grupo não serão mapeadas após o grupo ser excluído.

### Adicionando regras de grupo

É possível criar regras de grupo para que um grupo adicione dinamicamente objetos de storage, como volumes, clusters ou máquinas virtuais de armazenamento (SVMs) ao grupo. Você deve configurar pelo menos um grupo de condições com pelo menos uma condição para criar uma regra de grupo.

#### Antes de começar

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

Os objetos de armazenamento atualmente monitorados são adicionados assim que a regra de grupo é criada. Novos objetos são adicionados somente após o ciclo de monitoramento ser concluído.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **regras de grupo**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar regra de grupo**, especifique um nome para a regra de grupo.
4. No campo **Target Object Type** (tipo de objeto de destino), selecione o tipo de objeto de armazenamento que deseja agrupar.
5. No campo **Grupo**, selecione o grupo necessário para o qual deseja criar regras de grupo.

6. Na seção **condições**, execute as etapas a seguir para criar uma condição, um grupo de condições ou ambos:

Para criar	Faça isso...
Uma condição	<ol style="list-style-type: none"> <li>Selecione um operando na lista de operandos.</li> <li>Selecione <b>contains</b> ou <b>is</b> como operador.</li> <li>Introduza um valor ou selecione um valor na lista disponível.</li> </ol>
Um grupo de condição	<ol style="list-style-type: none"> <li>Clique em <b>Add Condition Group</b> (Adicionar grupo de condições)</li> <li>Selecione um operando na lista de operandos.</li> <li>Selecione <b>contains</b> ou <b>is</b> como operador.</li> <li>Introduza um valor ou selecione um valor na lista disponível.</li> <li>Clique em <b>Adicionar condição</b> para criar mais condições, se necessário, e repita as etapas de a a d para cada condição.</li> </ol>

7. Clique em **Add**.

#### Exemplo para criar uma regra de grupo

Execute as etapas a seguir na caixa de diálogo Adicionar regra de grupo para criar uma regra de grupo, incluindo a configuração de uma condição e a adição de um grupo de condições:

#### Passos

- Especifique um nome para a regra de grupo.
- Selecione o tipo de objeto como máquina virtual de storage (SVM).
- Selecione um grupo na lista de grupos.
- Na seção condições, selecione **Nome do objeto** como o operando.
- Selecione **contains** como operador.
- Introduza o valor `svm_data` como .
- Clique em **Adicionar grupo de condições**.
- Selecione **Nome do objeto** como o operando.
- Selecione **contains** como operador.
- Introduza o valor `vol` como .
- Clique em **Adicionar condição**.
- Repita os passos 8 a 10 selecionando **data-priority** como operando na etapa 8, **is** como operador na etapa 9 e **Critical** como o valor na etapa 10.
- Clique em **Add** para criar a condição para a regra de grupo.



## Editando regras de grupo

Você pode editar regras de grupo para modificar os grupos de condição e as condições dentro de um grupo de condições para adicionar ou remover objetos de armazenamento de ou para um grupo específico.

### Antes de começar

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

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **regras de grupo**, selecione a regra de grupo que deseja editar e clique em **Editar**.
3. Na caixa de diálogo **Editar regra de grupo**, altere o nome da regra de grupo, o nome do grupo associado, os grupos de condição e as condições conforme necessário.



Não é possível alterar o tipo de objeto de destino para uma regra de grupo.

4. Clique em **Salvar**.

## Eliminar regras de grupo

Você pode excluir uma regra de grupo do Active IQ Unified Manager quando a regra de grupo não for mais necessária.

### Antes de começar

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

Quando uma regra de grupo é excluída, os objetos de armazenamento associados serão removidos do grupo.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **regras de grupo**, selecione a regra de grupo que deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

## Adicionando ações de grupo

Você pode configurar ações de grupo que deseja aplicar a objetos de armazenamento em um grupo. A configuração de ações para um grupo permite economizar tempo, porque você não precisa adicionar essas ações a cada objeto individualmente.

### Antes de começar

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

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **ações de grupo**, clique em **Adicionar**.
3. Na caixa de diálogo **Add Group Action** (Adicionar ação de grupo), insira um nome e uma descrição para a ação.

4. No menu **Group** (Grupo), selecione um grupo para o qual deseja configurar a ação.
5. No menu **tipo de ação**, selecione um tipo de ação.

A caixa de diálogo expande-se, permitindo-lhe configurar o tipo de ação selecionado com os parâmetros necessários.

6. Insira os valores apropriados para os parâmetros necessários para configurar uma ação de grupo.
7. Clique em **Add**.

### **Editando ações de grupo**

Você pode editar os parâmetros de ação do grupo configurados no Unified Manager, como nome da ação do grupo, descrição, nome do grupo associado e parâmetros do tipo de ação.

#### **Antes de começar**

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

#### **Passos**

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **ações de grupo**, selecione a ação de grupo que deseja editar e clique em **Editar**.
3. Na caixa de diálogo **Editar ação de grupo**, altere o nome da ação de grupo, a descrição, o nome do grupo associado e os parâmetros do tipo de ação, conforme necessário.
4. Clique em **Salvar**.

### **Configuração dos limites de integridade do volume para grupos**

Você pode configurar limites de integridade do volume em nível de grupo para capacidade, cópias Snapshot, cotas de qtree, crescimento e inodes.

#### **Antes de começar**

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

O tipo de limite de integridade do volume de ação de grupo é aplicado apenas em volumes de um grupo.

#### **Passos**

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **ações de grupo**, clique em **Adicionar**.
3. Introduza um nome e uma descrição para a ação do grupo.
4. Na caixa suspensa **Grupo**, selecione um grupo para o qual deseja configurar a ação de grupo.
5. Selecione **Action Type** como o limite de integridade do volume.
6. Selecione a categoria para a qual deseja definir o limite.
7. Introduza os valores necessários para o limiar de saúde.
8. Clique em **Add**.

## Eliminar ações de grupo

Você pode excluir uma ação de grupo do Unified Manager quando a ação de grupo não for mais necessária.

### Antes de começar

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

Quando você exclui a ação de grupo para o limite de integridade do volume, os limites globais são aplicados aos objetos de storage nesse grupo. Quaisquer limites de integridade no nível do objeto definidos no objeto de storage não são afetados.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **ações de grupo**, selecione a ação de grupo que deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

## Reordenar ações de grupo

Você pode alterar a ordem das ações de grupo que devem ser aplicadas aos objetos de armazenamento em um grupo. As ações de grupo são aplicadas a objetos de armazenamento sequencialmente com base em sua classificação. A classificação mais baixa é atribuída à ação de grupo que você configurou por último. Você pode alterar a classificação da ação do grupo dependendo de seus requisitos.

### Antes de começar

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

Você pode selecionar uma única linha ou várias linhas e, em seguida, executar várias operações de arrastar e soltar para alterar a classificação das ações de grupo. No entanto, você deve salvar as alterações para que a nova priorização seja refletida na grade de ações do grupo.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > grupos**.
2. Na guia **ações de grupo**, clique em **Reordenar**.
3. Na caixa de diálogo **Reordenar ações de grupo**, arraste e solte as linhas para reorganizar a sequência de ações de grupo conforme necessário.
4. Clique em **Salvar**.

## Priorizando eventos de objetos de armazenamento usando anotações

Você pode criar e aplicar regras de anotação a objetos de armazenamento para que você possa identificar e filtrar esses objetos com base no tipo de anotação aplicada e sua prioridade.

### Compreender mais sobre anotações

Entender os conceitos sobre anotações ajuda você a gerenciar os eventos relacionados aos objetos de armazenamento em seu ambiente.

## Quais são as anotações

Uma anotação é uma cadeia de texto (o nome) que é atribuída a outra cadeia de texto (o valor). Cada par de nome-valor de anotação pode ser dinamicamente associado a objetos de armazenamento utilizando regras de anotação. Quando você associa objetos de armazenamento a anotações predefinidas, você pode filtrar e exibir os eventos relacionados a eles. É possível aplicar anotações a clusters, volumes e máquinas virtuais de storage (SVMs).

Cada nome de anotação pode ter vários valores; cada par de nome-valor pode ser associado a um objeto de armazenamento através de regras.

Por exemplo, você pode criar uma anotação chamada "data-center" com os valores "Boston" e "Canadá". Você pode então aplicar a anotação "data-center" com o valor "Boston" ao volume v1. Quando um alerta é gerado para qualquer evento em um volume v1 que é anotado com "data-center", o e-mail gerado indica a localização do volume, "Boston", e isso permite que você priorize e resolva o problema.

## Como as regras de anotação funcionam no Unified Manager

Uma regra de anotação é um critério que você define para anotar objetos de armazenamento (volumes, clusters ou máquinas virtuais de armazenamento (SVMs)). Pode utilizar grupos de condições ou condições para definir regras de anotação.

- Tem de associar uma regra de anotação a uma anotação.
- Você deve associar um tipo de objeto para uma regra de anotação; apenas um tipo de objeto pode ser associado a uma regra de anotação.
- O Unified Manager adiciona ou remove anotações de objetos de armazenamento após cada ciclo de monitoramento ou quando uma regra é criada, editada, excluída ou reordenada.
- Uma regra de anotação pode ter um ou mais grupos de condições e cada grupo de condições pode ter uma ou mais condições.
- Objetos de armazenamento podem ter várias anotações. Uma regra de anotação para uma anotação específica também pode usar anotações diferentes nas condições da regra para adicionar outra anotação a objetos já anotados.

## Condições

Você pode criar vários grupos de condições e cada grupo de condições pode ter uma ou mais condições. Pode aplicar todos os grupos de condições definidos numa regra de anotação de uma anotação para anotar objetos de armazenamento.

As condições dentro de um grupo de condições são executadas usando LÓGICA e. Todas as condições de um grupo de condições devem ser atendidas. Quando você cria ou modifica uma regra de anotação, uma condição é criada que aplica, seleciona e anota somente os objetos de armazenamento que atendem a todas as condições no grupo condição. Você pode usar várias condições dentro de um grupo de condições quando quiser restringir o escopo de quais objetos de armazenamento anotar.

Você pode criar condições com objetos de armazenamento usando os seguintes operandos e operador e especificando o valor necessário.

Tipo de objeto de storage	Operandos aplicáveis
Volume	<ul style="list-style-type: none"> <li>• Nome do objeto</li> <li>• Nome do cluster proprietário</li> <li>• Possuir nome SVM</li> <li>• Anotações</li> </ul>
SVM	<ul style="list-style-type: none"> <li>• Nome do objeto</li> <li>• Nome do cluster proprietário</li> <li>• Anotações</li> </ul>
Cluster	<ul style="list-style-type: none"> <li>• Nome do objeto</li> <li>• Anotações</li> </ul>

Quando você seleciona a anotação como um operando para qualquer objeto de armazenamento, o operador "is" está disponível. Para todos os outros operandos, você pode selecionar "is" ou "contains" como operador. Quando você seleciona o operador "is", a condição é avaliada para uma correspondência exata do valor do operando com o valor fornecido para o operando selecionado. Quando você seleciona o operador "contém", a condição é avaliada para atender a um dos seguintes critérios:

- O valor do operando é uma correspondência exata com o valor do operando selecionado.
- O valor do operando contém o valor fornecido para o operando selecionado.

### Exemplo de uma regra de anotação com condições

Considere uma regra de anotação com um grupo de condições para um volume com as duas seguintes condições:

- O nome contém "vol"
- O nome da SVM é "dATA\_svm"

Esta regra de anotação anota todos os volumes que incluem "vol" em seus nomes e que são hospedados em SVMs com o nome "dATA\_svm" com a anotação selecionada e o tipo de anotação.

### Grupos de condições

Os grupos de condição são executados usando OU lógico e, em seguida, aplicados a objetos de armazenamento. Os objetos de armazenamento devem atender aos requisitos de um dos grupos de condições a serem anotados. Os objetos de armazenamento que atendem às condições de todos os grupos de condições são anotados. Você pode usar grupos de condições para aumentar o escopo dos objetos de armazenamento a serem anotados.

### Exemplo de uma regra de anotação com grupos de condições

Considere uma regra de anotação com dois grupos de condições para um volume; cada grupo contém as seguintes duas condições:

- Grupo de condições 1

- O nome contém "vol"
- O nome do SVM é "dATA\_svm" este grupo de condições anota todos os volumes que incluem "'vol'" em seus nomes e que são hospedados em svms com o nome "dATA\_svm".
- Grupo de condições 2
  - O nome contém "vol"
  - O valor de anotação da prioridade de dados é "crítico". Este grupo de condições anotou todos os volumes que incluem "'vol'" em seus nomes e que são anotados com o valor de anotação de prioridade de dados como "crítico".

Quando uma regra de anotação contendo esses dois grupos de condições é aplicada em objetos de armazenamento, os seguintes objetos de armazenamento são anotados:

- Todos os volumes que incluem "'vol'" em seus nomes e que são hospedados no SVM com o nome "dATA\_svm".
- Todos os volumes que incluem "'vol'" em seus nomes e que são anotados com o valor de anotação de prioridade de dados como "crítico".

#### Descrição dos valores de anotação predefinidos

**Prioridade de dados** é uma anotação predefinida que tem os valores Missão crítica, alta e baixa. Esses valores permitem anotar objetos de armazenamento com base na prioridade dos dados que eles contêm. Não é possível editar ou eliminar os valores de anotação predefinidos.

- **Prioridade de dados: Missão crítica**

Esta anotação é aplicada a objetos de armazenamento que contêm dados de missão crítica. Por exemplo, objetos que contêm aplicações de produção podem ser considerados de missão crítica.

- **Prioridade de dados: Alta**

Esta anotação é aplicada a objetos de armazenamento que contêm dados de alta prioridade. Por exemplo, objetos que hospedam aplicativos de negócios podem ser considerados de alta prioridade.

- **Prioridade de dados: Baixa**

Esta anotação é aplicada a objetos de armazenamento que contêm dados de baixa prioridade. Por exemplo, os objetos que estão em armazenamento secundário, como destinos de backup e espelhamento, podem ser de baixa prioridade.

#### Adicionar anotações dinamicamente

Ao criar anotações personalizadas, o Unified Manager associa dinamicamente clusters, máquinas virtuais de armazenamento (SVMs) e volumes às anotações usando regras. Essas regras atribuem automaticamente as anotações a objetos de armazenamento.

#### Antes de começar

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

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na página **Anotações**, clique em **Add Annotation**.
3. Na caixa de diálogo **Add Annotation** (Adicionar anotação), digite um nome e uma descrição para a anotação.
4. Opcional: Na seção **valores de anotação**, clique em **Adicionar** para adicionar valores à anotação.
5. Clique em **Salvar**.

### Adicionar valores a anotações

Você pode adicionar valores a anotações e, em seguida, associar objetos de armazenamento a um par de nome-valor de anotação específico. Adicionar valores a anotações ajuda a gerenciar objetos de armazenamento de forma mais eficaz.

#### Antes de começar

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

Não é possível adicionar valores a anotações predefinidas.

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na página **Anotações**, selecione a anotação à qual deseja adicionar um valor e clique em **Add** na seção **values**.
3. Na caixa de diálogo **Add Annotation value** (Adicionar valor de anotação), especifique um valor para a anotação.

O valor que especificar tem de ser exclusivo para a anotação selecionada.

4. Clique em **Add**.

### Eliminar anotações

Você pode excluir anotações personalizadas e seus valores quando não forem mais necessários.

#### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Os valores de anotação não devem ser utilizados noutras anotações ou regras de grupo.

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. No separador **Anotações**, selecione a anotação que pretende eliminar.

São apresentados os detalhes da anotação selecionada.

3. Clique em **ações > Excluir** para excluir a anotação selecionada e seu valor.
4. Na caixa de diálogo de aviso, clique em **Yes** para confirmar a exclusão.

## Visualizar a lista de anotações e detalhes

É possível exibir a lista de anotações associadas dinamicamente a clusters, volumes e máquinas virtuais de storage (SVMs). Você também pode exibir detalhes como a descrição, criada por, data criada, valores, regras e os objetos associados à anotação.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. No separador **Anotações**, clique no nome da anotação para ver os detalhes associados.

## Eliminar valores de anotações

Pode eliminar valores associados a anotações personalizadas quando esse valor já não se aplica à anotação.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- O valor da anotação não deve estar associado a quaisquer regras de anotação ou regras de grupo.

Não é possível eliminar valores de anotações predefinidas.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na lista de anotações no separador **Anotações**, selecione a anotação a partir da qual pretende eliminar um valor.
3. Na área **valores** da guia **Anotações**, selecione o valor que deseja excluir e clique em **Excluir**.
4. Na caixa de diálogo **Aviso**, clique em **Sim**.

O valor é eliminado e já não é apresentado na lista de valores para a anotação selecionada.

## Criando regras de anotação

Você pode criar regras de anotação que o Unified Manager usa para anotar dinamicamente objetos de armazenamento, como volumes, clusters ou máquinas virtuais de armazenamento (SVMs).

### Antes de começar

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

Os objetos de armazenamento atualmente monitorizados são anotados assim que a regra de anotação é criada. Os novos objetos são anotados apenas após o ciclo de monitorização ser concluído.

### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na guia **regras de anotação**, clique em **Adicionar**.
3. Na caixa de diálogo **Add Annotation Rule** (Adicionar regra de anotação), especifique um nome para a regra de anotação.
4. No campo **Target Object Type** (tipo de objeto de destino), selecione o tipo de objeto de armazenamento



que deseja anotar.

5. Nos campos **Apply Annotation** (aplicar anotação), selecione o valor de anotação e anotação que pretende utilizar.
6. Na seção condições, execute a ação apropriada para criar uma condição, um grupo de condições ou ambos:

Para criar...	Faça isso...
Uma condição	<ol style="list-style-type: none"><li>a. Selecione um operando na lista de operandos.</li><li>b. Selecione <b>contains</b> ou <b>is</b> como operador.</li><li>c. Introduza um valor ou selecione um valor na lista disponível.</li></ol>
Um grupo de condição	<ol style="list-style-type: none"><li>a. Clique em <b>Add Condition Group</b> (Adicionar grupo de condições).</li><li>b. Selecione um operando na lista de operandos.</li><li>c. Selecione <b>contains</b> ou <b>is</b> como operador.</li><li>d. Introduza um valor ou selecione um valor na lista disponível.</li><li>e. Clique em <b>Adicionar condição</b> para criar mais condições, se necessário, e repita as etapas de a a d para cada condição.</li></ol>

7. Clique em **Add**.

#### Exemplo de criação de uma regra de anotação

Execute as seguintes etapas na caixa de diálogo Adicionar regra de anotação para criar uma regra de anotação, incluindo configurar uma condição e adicionar um grupo de condições:

#### Passos

1. Especifique um nome para a regra de anotação.
2. Selecione o tipo de objeto de destino como máquina virtual de storage (SVM).
3. Selecione uma anotação na lista de anotações e especifique um valor.
4. Na seção condições, selecione **Nome do objeto** como o operando.
5. Selecione **contains** como operador.
6. Introduza o valor `svm_data` como .
7. Clique em **Adicionar grupo de condições**.
8. Selecione **Nome do objeto** como o operando.
9. Selecione **contains** como operador.
10. Introduza o valor `vol` como .
11. Clique em **Adicionar condição**.
12. Repita os passos 8 a 10 selecionando **data-priority** como o operando na etapa 8, **is** como o operador na etapa 9 e **Mission-critical** como o valor na etapa 10.

13. Clique em **Add**.

### Adicionar anotações manualmente a objetos de armazenamento individuais

Você pode anotar manualmente volumes, clusters e SVMs selecionados sem usar regras de anotação. Você pode anotar um único objeto de armazenamento ou vários objetos de armazenamento e especificar a combinação de par de nome-valor necessária para a anotação.

#### Antes de começar

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

#### Passos

1. Navegue até os objetos de armazenamento que deseja anotar:

Para adicionar anotação a...	Faça isso...
Clusters	a. Clique em <b>Storage &gt; clusters</b> . b. Selecione um ou mais clusters.
Volumes	a. Clique em <b>Storage &gt; volumes</b> . b. Selecione um ou mais volumes.
SVMs	a. Clique em <b>Storage &gt; SVMs</b> . b. Selecione um ou mais SVMs.

2. Clique em **Annotate** e selecione um par de nome-valor.

3. Clique em **aplicar**.

### Editar regras de anotação

Pode editar regras de anotação para modificar os grupos de condições e condições dentro do grupo de condições para adicionar anotações ou remover anotações de objetos de armazenamento.

#### Antes de começar

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

As anotações são dissociadas de objetos de armazenamento quando você edita as regras de anotação associadas.

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.

2. Na guia **regras de anotação**, selecione a regra de anotação que deseja editar e clique em **ações > Editar**.

3. Na caixa de diálogo **Edit Annotation Rule** (Editar regra de anotação), altere o nome da regra, o nome e o valor da anotação, os grupos de condição e as condições conforme necessário.

Não é possível alterar o tipo de objeto alvo para uma regra de anotação.

4. Clique em **Salvar**.

### Configurar condições para regras de anotação

Você pode configurar uma ou mais condições para criar regras de anotação que o Unified Manager aplica aos objetos de armazenamento. Os objetos de armazenamento que satisfazem a regra de anotação são anotados com o valor especificado na regra.

#### Antes de começar

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

#### Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na guia **regras de anotação**, clique em **Adicionar**.
3. Na caixa de diálogo **Add Annotation Rule** (Adicionar regra de anotação), insira um nome para a regra.
4. Selecione um tipo de objeto na lista Target Object Type (tipo de objeto alvo) e, em seguida, selecione um nome e um valor de anotação na lista.
5. Na seção **condições** da caixa de diálogo, selecione um operando e um operador na lista e insira um valor de condição ou clique em **Adicionar condição** para criar uma nova condição.
6. Clique em **Salvar e Adicionar**.

#### Exemplo de configuração de uma condição para uma regra de anotação

Considere uma condição para o tipo de objeto SVM, onde o nome do objeto contém "svm\_data".

Execute as seguintes etapas na caixa de diálogo Adicionar regra de anotação para configurar a condição:

#### Passos

1. Introduza um nome para a regra de anotação.
2. Selecione o tipo de objeto de destino como SVM.
3. Selecione uma anotação na lista de anotações e um valor.
4. No campo **condições**, selecione **Nome do objeto** como operando.
5. Selecione **contains** como operador.
6. Introduza o valor `svm_data` como .
7. Clique em **Add**.

### Eliminar regras de anotação

Pode eliminar regras de anotação do Active IQ Unified Manager quando as regras já não forem necessárias.

#### Antes de começar

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

Quando elimina uma regra de anotação, a anotação é desassociada e removida dos objetos de armazenamento.

## Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na guia **regras de anotação**, selecione a regra de anotação que deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, clique em **Sim** para confirmar a exclusão.

## Reordenar regras de anotação

Você pode alterar a ordem na qual o Unified Manager aplica regras de anotação a objetos de armazenamento. As regras de anotação são aplicadas a objetos de armazenamento sequencialmente com base em sua classificação. Quando você configura uma regra de anotação, a classificação é menor. Mas você pode alterar a classificação da regra de anotação dependendo de seus requisitos.

### Antes de começar

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

Você pode selecionar uma única linha ou várias linhas e executar muitas operações de arrastar e soltar para alterar a classificação das regras de anotação. No entanto, você deve salvar as alterações para que a repriorização seja exibida na guia regras de anotação.

## Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na guia **regras de anotação**, clique em **Reordenar**.
3. Na caixa de diálogo **regra de anotação de reordenação**, arraste e solte linhas simples ou múltiplas para reorganizar a sequência das regras de anotação.
4. Clique em **Salvar**.

Tem de guardar as alterações para que a reordenação seja apresentada.

## Envio de um pacote de suporte por meio da IU da Web e do console de manutenção

Você deve enviar um pacote de suporte quando o problema que você tem exigir diagnóstico e solução de problemas mais detalhados do que uma mensagem AutoSupport fornece. Você pode enviar um pacote de suporte ao suporte técnico usando a IU da Web e o console de manutenção do Unified Manager.

O Unified Manager armazena, no máximo, dois pacotes de suporte completos e três pacotes de suporte leve ao mesmo tempo.

### Informações relacionadas

["Funções e recursos de usuário do Unified Manager"](#)

### Envio de mensagens AutoSupport e pacotes de suporte para o suporte técnico

A página do AutoSupport permite enviar mensagens AutoSupport predefinidas e sob demanda para sua equipe de suporte técnico, a fim de garantir uma operação correta do

seu ambiente e ajudá-lo a manter a integridade do seu ambiente. O AutoSupport está habilitado por padrão e não deve ser desativado, para que você receba os benefícios do NetAppactive IQ.

Você pode enviar informações do sistema de diagnóstico e dados detalhados sobre o servidor do Unified Manager em uma mensagem como e quando necessário, agendar uma mensagem para ser enviada periodicamente ou até mesmo gerar e enviar pacotes de suporte para a equipe de suporte técnico.



Um usuário com função de administrador de storage pode gerar e enviar mensagens AutoSupport sob demanda e pacotes de suporte para o suporte técnico. No entanto, somente um administrador ou usuário de manutenção pode ativar ou desativar o AutoSupport periódico e configurar as configurações HTTP conforme descrito na seção Configuração do servidor proxy HTTP. Em um ambiente que precisa usar um servidor proxy HTTP, a configuração deve ser concluída antes que um administrador de armazenamento possa enviar mensagens AutoSupport sob demanda e pacotes de suporte para suporte técnico.

#### Envio de mensagens AutoSupport sob demanda

Você pode gerar e enviar uma mensagem sob demanda para o suporte técnico, para um destinatário de e-mail especificado ou para ambos.

#### Passos

1. Navegue até **Geral > AutoSupport** e execute uma ou ambas as seguintes ações:
2. Se quiser enviar a mensagem AutoSupport para o suporte técnico, marque a caixa de seleção **Enviar para o suporte técnico**.
3. Se quiser enviar a mensagem AutoSupport para um destinatário de e-mail específico, marque a caixa de seleção **Enviar para destinatário de e-mail** e insira o endereço de e-mail do destinatário.
4. Clique em **Salvar**.
5. Clique em **Generate and Send AutoSupport**.

#### Habilitando o AutoSupport periódico

Você pode enviar mensagens específicas e predefinidas para o suporte técnico para diagnóstico e resolução de problemas periodicamente. Esta funcionalidade está ativada por predefinição. Se estiver desativado, um administrador ou utilizador de manutenção pode ativar as definições.

#### Passos

1. Navegue até **Geral > AutoSupport**.
2. Na seção AutoSupport Periódico, marque a caixa de seleção **Ativar envio periódico de dados AutoSupport para Active IQ**.
3. Se necessário, defina o nome, a porta e as informações de autenticação para o servidor proxy HTTP, conforme descrito na seção Configuração do servidor proxy HTTP.
4. Clique em **Salvar**.

#### Carregar pacote de suporte sob demanda

Você pode gerar e enviar um pacote de suporte para o suporte técnico com base no requisito de solução de problemas. O Unified Manager armazena apenas os dois pacotes de suporte gerados mais recentemente. Pacotes de suporte mais antigos são excluídos do sistema.

Como alguns tipos de dados de suporte podem usar uma grande quantidade de recursos de cluster ou levar muito tempo para serem concluídos, ao selecionar o pacote de suporte completo, você pode incluir ou excluir tipos de dados específicos para reduzir o tamanho do pacote de suporte. Você também tem a opção de criar um pacote de suporte leve que contém apenas 30 dias de Registros e Registros de banco de dados de configuração — exclui dados de desempenho, arquivos de gravação de aquisição e despejo de heap do servidor.

### Passos

1. Navegue até **Geral > AutoSupport**.
2. Na seção Pacote de suporte sob demanda, clique em **Generate and Send Support Bundle**.
3. Para enviar um pacote de suporte leve ao suporte técnico, no pop-up Generate and Send Support Bundle, marque a caixa de seleção Generate light support bundle\*\* (gerar e enviar pacote de suporte leve).
4. Como alternativa, para enviar um pacote de suporte completo, marque a caixa de seleção **Generate full support bundle** (gerar pacote de suporte completo). Selecione os tipos de dados específicos a incluir ou excluir no pacote de suporte.



Mesmo que você não selecione nenhum tipo de dados, o pacote de suporte ainda será gerado com outros dados do Unified Manager.

5. Marque a caixa de seleção **Enviar o pacote para suporte técnico** para gerar e enviar o pacote para suporte técnico. Se você não selecionar essa caixa de seleção, o pacote será gerado e armazenado localmente no servidor do Unified Manager. O pacote de suporte gerado está disponível para uso posterior no diretório /support em sistemas VMware, em /opt/netapp/data/support/ sistemas Linux e em ProgramData\NetApp\OnCommandAppData\ocum\support sistemas Windows.
6. Clique em **Enviar**.

### Configurando o servidor proxy HTTP

Você pode designar um proxy para fornecer acesso à Internet para enviar conteúdo do AutoSupport para suporte se o seu ambiente não fornecer acesso direto do servidor do Gerenciador Unificado. Esta seção está disponível apenas para usuários de administrador e manutenção.

#### • Use proxy HTTP

Marque esta caixa para identificar o servidor que está sendo usado como proxy HTTP.

Insira o nome do host ou o endereço IP do servidor proxy e o número da porta usada para se conectar ao servidor.

#### • Use autenticação

Marque esta caixa se precisar fornecer informações de autenticação para acessar o servidor que está sendo usado como proxy HTTP.

Introduza o nome de utilizador e a palavra-passe necessários para a autenticação com o proxy HTTP.



Os proxies HTTP que fornecem somente a Autenticação básica não são suportados.

### Aceder à consola de manutenção

Se a interface de usuário do Unified Manager não estiver em operação ou se for

necessário executar funções que não estejam disponíveis na interface do usuário, você poderá acessar o console de manutenção para gerenciar o sistema do Unified Manager.

### Antes de começar

Você precisa ter instalado e configurado o Unified Manager.

Após 15 minutos de inatividade, o console de manutenção faz o logout.



Quando instalado no VMware, se você já fez login como usuário de manutenção pelo console VMware, não será possível fazer login simultaneamente usando o Secure Shell.

### Passo

1. Siga estas etapas para acessar o console de manutenção:

Neste sistema operativo...	Siga estes passos...
VMware	<ol style="list-style-type: none"><li>Usando o Secure Shell, conete-se ao endereço IP ou ao nome de domínio totalmente qualificado do dispositivo virtual do Unified Manager.</li><li>Inicie sessão na consola de manutenção utilizando o nome de utilizador e a palavra-passe de manutenção.</li></ol>
Linux	<ol style="list-style-type: none"><li>Usando o Secure Shell, conete-se ao endereço IP ou ao nome de domínio totalmente qualificado do sistema Unified Manager.</li><li>Inicie sessão no sistema com o nome e a palavra-passe do utilizador de manutenção (umadmin).</li><li>Digite o comando <code>maintenance_console</code> e pressione Enter.</li></ol>
Windows	<ol style="list-style-type: none"><li>Faça login no sistema Unified Manager com credenciais de administrador.</li><li>Inicie o PowerShell como administrador do Windows.</li><li>Digite o comando <code>maintenance_console</code> e pressione Enter.</li></ol>

O menu do console de manutenção do Unified Manager é exibido.

### Gerando e carregando um pacote de suporte

Você pode gerar um pacote de suporte, contendo informações de diagnóstico, para que possa enviá-lo ao suporte técnico para obter ajuda na solução de problemas.

A partir do Unified Manager 9,8, se o servidor do Unified Manager estiver conectado à Internet, você também

poderá fazer o upload do pacote de suporte para o NetApp a partir do console de manutenção.

### Antes de começar

Você deve ter acesso ao console de manutenção como usuário de manutenção.

Como alguns tipos de dados de suporte podem usar uma grande quantidade de recursos de cluster ou levar muito tempo para serem concluídos, ao selecionar o pacote de suporte completo, você pode especificar tipos de dados a serem incluídos ou excluídos para reduzir o tamanho do pacote de suporte. Você também tem a opção de criar um pacote de suporte leve que contém apenas 30 dias de Registros e Registros de banco de dados de configuração — exclui dados de desempenho, arquivos de gravação de aquisição e despejo de heap do servidor.

O Unified Manager armazena apenas os dois pacotes de suporte gerados mais recentemente. Pacotes de suporte mais antigos são excluídos do sistema.

### Passos

1. No console de manutenção **Menu Principal**, selecione **suporte/Diagnóstico**.
2. Selecione **Generate Light Support Bundle** ou **Generate Support Bundle** dependendo do nível de detalhes que você deseja ter no pacote de suporte.
3. Se você escolher o pacote de suporte completo, marque ou desmarque os seguintes tipos de dados para incluir ou excluir no pacote de suporte:

- **despejo de banco de dados**

Um despejo do banco de dados do MySQL Server.

- **despejo de pilha**

Um instantâneo do estado dos principais processos do servidor do Unified Manager. Esta opção está desativada por predefinição e deve ser selecionada apenas quando solicitado pelo apoio ao cliente.

- **gravações de aquisição**

Gravação de todas as comunicações entre o Unified Manager e os clusters monitorados.



Se você desmarcar todos os tipos de dados, o pacote de suporte ainda será gerado com outros dados do Unified Manager.

4. Digite ``g`` e pressione Enter para gerar o pacote de suporte.

Como a geração de um pacote de suporte é uma operação com uso intenso de memória, você será solicitado a verificar se você tem certeza de que deseja gerar o pacote de suporte neste momento.

5. Digite ``y`` e pressione Enter para gerar o pacote de suporte.

Se você não quiser gerar o pacote de suporte neste momento, digite `n` e pressione Enter.

6. Se você incluiu arquivos de despejo de banco de dados no pacote de suporte completo, será solicitado que você especifique o período de tempo para o qual deseja incluir estatísticas de desempenho. Incluir estatísticas de desempenho pode levar muito tempo e espaço, para que você também possa despejar o banco de dados sem incluir estatísticas de desempenho:

- a. Introduza a data de início no formato YYYYMMDD.



Por exemplo, digite 20210101 para 1 de janeiro de 2021. Insira `n` se você não quiser que as estatísticas de desempenho sejam incluídas.

- b. Introduza o número de dias de estatísticas a incluir, a partir das 12 horas da data de início especificada.

Pode introduzir um número de 1 a 10.

Se você estiver incluindo estatísticas de desempenho, o sistema exibirá o período de tempo para o qual as estatísticas de desempenho serão coletadas.

7. Depois que o pacote de suporte for criado, você será solicitado a enviá-lo para o NetApp. Digite ``y`` e pressione Enter.

Você será solicitado a inserir o número do caso de suporte.

8. Se já tiver um número de caso, introduza o número e prima Enter. Caso contrário, basta pressionar Enter.

O pacote de suporte é carregado para o NetApp.

Se o servidor do Unified Manager não estiver conectado à Internet ou se você não conseguir carregar o pacote de suporte por qualquer outro motivo, poderá recuperá-lo e enviá-lo manualmente. Você pode recuperá-lo usando um cliente SFTP ou usando comandos CLI UNIX ou Linux. Em instalações do Windows, você pode usar a Área de trabalho Remota (RDP) para recuperar o pacote de suporte.

O pacote de suporte gerado reside no diretório `/support` em sistemas VMware, em `/opt/NetApp/data/support/` em sistemas Linux, e no suporte a NetApp em sistemas Windows.

## Informações relacionadas

["Funções e recursos de usuário do Unified Manager"](#)

## Recuperar o pacote de suporte usando um cliente Windows

Se você for um usuário do Windows, poderá baixar e instalar uma ferramenta para recuperar o pacote de suporte do servidor do Unified Manager. Você pode enviar o pacote de suporte ao suporte técnico para obter um diagnóstico mais detalhado de um problema. FileZilla ou WinSCP são exemplos de ferramentas que você pode usar.

### Antes de começar

Você deve ser o usuário de manutenção para executar esta tarefa.

Você deve usar uma ferramenta que suporte SCP ou SFTP.

### Passos

1. Baixe e instale uma ferramenta para recuperar o pacote de suporte.
2. Abra a ferramenta.
3. Conecte-se ao seu servidor de gerenciamento do Unified Manager através de SFTP.

A ferramenta exibe o conteúdo do diretório `/support` e você pode visualizar todos os pacotes de suporte existentes.

4. Selecione o diretório de destino para o pacote de suporte que deseja copiar.
5. Selecione o pacote de suporte que deseja copiar e use a ferramenta para copiar o arquivo do servidor do Unified Manager para o sistema local.

### Recuperando o pacote de suporte usando um cliente UNIX ou Linux

Se você é um usuário UNIX ou Linux, você pode recuperar o pacote de suporte do seu vApp usando a interface de linha de comando (CLI) no servidor cliente Linux. Você pode usar SCP ou SFTP para recuperar o pacote de suporte.

#### Antes de começar

Você deve ser o usuário de manutenção para executar esta tarefa.

Você deve ter gerado um pacote de suporte usando o console de manutenção e ter o nome do pacote de suporte disponível.

#### Passos

1. Acesse a CLI através do Telnet ou do console, usando o servidor cliente Linux.
2. Acesse o `/support` diretório.
3. Recupere o pacote de suporte e copie-o para o diretório local usando o seguinte comando:

Se você estiver usando...	Em seguida, use o seguinte comando...
SCP	<code>scp &lt;maintenance-user&gt;@&lt;vApp-name-or-ip&gt;:/support/support_bundle_file_name.7z &lt;destination-directory&gt;</code>
SFTP	<code>sftp &lt;maintenance-user&gt;@&lt;vApp-name-or-ip&gt;:/support/support_bundle_file_name.7z &lt;destination-directory&gt;</code>

O nome do pacote de suporte é fornecido a você quando você o gera usando o console de manutenção.

4. Introduza a palavra-passe do utilizador de manutenção.

#### Exemplos

O exemplo a seguir usa SCP para recuperar o pacote de suporte:

```

`$ scp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `maintenance_user_password`
support_bundle_20160216_145359.7z 100% 119MB 11.9MB/s 00:10

```

O exemplo a seguir usa SFTP para recuperar o pacote de suporte:

```
`$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

## Envio de um pacote de suporte ao suporte técnico

Quando um problema requer informações de diagnóstico e solução de problemas mais detalhadas do que uma mensagem do AutoSupport fornece, você pode enviar um pacote de suporte para o suporte técnico.

### Antes de começar

Você precisa ter acesso ao pacote de suporte para enviá-lo ao suporte técnico.

Você deve ter um número de caso gerado através do site de suporte técnico.

### Passos

1. Faça login no site de suporte da NetApp.
2. Carregue o ficheiro.

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

## Tarefas e informações relacionadas a vários fluxos de trabalho

Algumas tarefas e textos de referência que podem ajudá-lo a entender e concluir um fluxo de trabalho são comuns a muitos fluxos de trabalho no Unified Manager, incluindo adicionar e revisar notas sobre um evento, atribuir um evento, reconhecer e resolver eventos, além de detalhes sobre volumes, máquinas virtuais de storage (SVMs), agregados e assim por diante.

### Componentes do cluster e por que eles podem estar na contenção

Você pode identificar problemas de desempenho do cluster quando um componente do cluster entra em contenção. O desempenho de workloads que usam o componente diminui e seu tempo de resposta (latência) para solicitações do cliente aumenta, o que aciona um evento no Unified Manager.

Um componente que está em disputa não pode funcionar em um nível ideal. Seu desempenho diminuiu e o desempenho de outros componentes e cargas de trabalho do cluster, chamados *vítimas*, pode ter aumentado a latência. Para sair da contenção de um componente, você precisa reduzir o workload ou aumentar a capacidade de lidar com mais trabalho, para que a performance possa retornar aos níveis normais. Como o Unified Manager coleta e analisa a performance do workload em intervalos de cinco minutos, ele detecta quando um componente do cluster é consistentemente sobreusado. Não são detectados picos transitórios de sobreutilização que duram apenas uma curta duração dentro do intervalo de cinco minutos.

Por exemplo, um agregado de storage pode estar sob contenção porque um ou mais workloads nele estão competindo para que suas solicitações de e/S sejam atendidas. Outras cargas de trabalho no agregado podem ser afetadas, fazendo com que seu desempenho diminua. Para reduzir a quantidade de atividade no agregado, há etapas diferentes, como mover uma ou mais workloads para um agregado ou nó menos ocupado, para diminuir a demanda geral de workload no agregado atual. Para um grupo de políticas de QoS, você pode ajustar o limite de taxa de transferência ou mover workloads para um grupo de políticas diferente, para que os workloads não fiquem mais sendo controlados.

O Unified Manager monitora os seguintes componentes do cluster para alertá-lo quando eles estão na contenção:

- **Rede**

Representa o tempo de espera das solicitações de e/S pelos protocolos de rede externos no cluster. O tempo de espera é o tempo gasto esperando que as transações "prontas para transferência" sejam concluídas antes que o cluster possa responder a uma solicitação de e/S. Se o componente de rede estiver em contenção, isso significa que o alto tempo de espera na camada de protocolo está impactando a latência de uma ou mais cargas de trabalho.

- **Processamento de rede**

Representa o componente de software no cluster envolvido com o processamento de e/S entre a camada de protocolo e o cluster. O processamento da rede de tratamento do nó pode ter sido alterado desde que o evento foi detectado. Se o componente de processamento de rede estiver em contenção, isso significa que a alta utilização no nó de processamento de rede está impactando a latência de uma ou mais cargas de trabalho.

Ao usar um cluster All SAN Array em uma configuração ativo-ativo, o valor de latência de processamento de rede é exibido para ambos os nós para que você possa verificar se os nós estão compartilhando a carga igualmente.

- **\* Limite de QoS Max\***

Representa a configuração de taxa de transferência máxima (pico) do grupo de políticas de qualidade do serviço (QoS) de storage atribuído ao workload. Se o componente do grupo de políticas estiver na contenção, isso significa que todas as cargas de trabalho no grupo de políticas estão sendo controladas pelo limite de taxa de transferência definido, o que está impactando a latência de uma ou mais dessas cargas de trabalho.

- **Limite de QoS min**

Representa a latência de um workload que está sendo causado pela configuração mínima (esperada) de taxa de transferência de QoS atribuída a outros workloads. Se o conjunto mínimo de QoS em certos workloads usar a maior parte da largura de banda para garantir a taxa de transferência prometida, outros workloads serão controlados e verão mais latência.

- **Interconexão de cluster**

Representa os cabos e adaptadores com os quais os nós em cluster estão fisicamente conectados. Se o componente de interconexão de cluster estiver na contenção, isso significa que o tempo de espera alto para solicitações de e/S na interconexão de cluster está impactando a latência de um ou mais workloads.

- **Data Processing**

Representa o componente de software no cluster envolvido com o processamento de e/S entre o cluster e

o agregado de storage que contém a carga de trabalho. O Data Processing de tratamento do nó pode ter sido alterado desde que o evento foi detetado. Se o componente Data Processing estiver em contenção, isso significa que a alta utilização no nó Data Processing está impactando a latência de um ou mais workloads.

- **\* Ativação de volume\***

Representa o processo que controla o uso de todos os volumes ativos. Em ambientes grandes onde mais de 1000 volumes estão ativos, esse processo controla quantos volumes críticos precisam acessar recursos por meio do nó ao mesmo tempo. Quando o número de volumes ativos simultâneos exceder o limite máximo recomendado, alguns dos volumes não críticos terão latência conforme identificado aqui.

- **Recursos MetroCluster**

Representa os recursos do MetroCluster, incluindo NVRAM e links interswitches (ISLs), usados para espelhar dados entre clusters em uma configuração do MetroCluster. Se o componente MetroCluster estiver em contenção, isso significa que a alta taxa de transferência de gravação de workloads no cluster local ou um problema de integridade de link está impactando a latência de um ou mais workloads no cluster local. Se o cluster não estiver em uma configuração do MetroCluster, este ícone não será exibido.

- **Operações agregadas ou SSD agregadas**

Representa o agregado de storage no qual os workloads estão sendo executados. Se o componente agregado estiver na contenção, isso significa que a alta utilização no agregado está impactando a latência de um ou mais workloads. Um agregado consiste em todos os HDDs, ou uma combinação de HDDs e SSDs (agregado de Flash Pool), ou uma combinação de HDDs e uma camada de nuvem (agregado de FabricPool). Um "agregado SSD" consiste em todos os SSDs (um agregado all-flash) ou uma combinação de SSDs e uma camada de nuvem (agregado FabricPool).

- **Latência da nuvem**

Representa o componente de software no cluster envolvido com o processamento de e/S entre o cluster e a camada de nuvem na qual os dados do usuário são armazenados. Se o componente de latência da nuvem estiver em contenção, isso significa que uma grande quantidade de leituras de volumes hospedados na camada de nuvem está impactando a latência de um ou mais workloads.

- **Sincronizar SnapMirror**

Representa o componente de software no cluster envolvido com a replicação dos dados do usuário do volume primário para o volume secundário em uma relação síncrona do SnapMirror. Se o componente Sync SnapMirror estiver na contenção, isso significa que a atividade das operações síncronas do SnapMirror está impactando a latência de um ou mais workloads.

## **Página de detalhes de volume / Saúde**

Pode utilizar a página de detalhes de volume / Saúde para ver informações detalhadas sobre um volume selecionado, como capacidade, eficiência de armazenamento, configuração, proteção, anotação e eventos gerados. Você também pode exibir informações sobre os objetos relacionados e alertas relacionados para esse volume.

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

## Botões de comando

Os botões de comando permitem executar as seguintes tarefas para o volume selecionado:

- **Mude para a visualização de desempenho**

Permite-lhe navegar para a página de detalhes de volume / desempenho.

- **Ações**

- Adicionar alerta

Permite adicionar um alerta ao volume selecionado.

- Editar limites

Permite modificar as definições de limite para o volume selecionado.

- Anotar

Permite anotar o volume selecionado.

- Proteger

Permite criar relações SnapMirror ou SnapVault para o volume selecionado.

- Relação

Permite executar as seguintes operações de relação de proteção:

- Editar

Inicia a caixa de diálogo Editar relacionamento, que permite alterar políticas, programações e taxas de transferência máximas existentes do SnapMirror para um relacionamento de proteção existente.

- Abortar

Aborta transferências que estão em andamento para um relacionamento selecionado. Opcionalmente, ele permite que você remova o ponto de verificação de reinicialização para transferências que não sejam a transferência de linha de base. Não é possível remover o ponto de verificação para uma transferência de linha de base.

- Quiesce

Desativa temporariamente as atualizações agendadas para uma relação selecionada. As transferências que já estão em andamento devem ser concluídas antes que o relacionamento seja interrompido.

- Pausa

Quebra a relação entre os volumes de origem e destino e altera o destino para um volume de leitura e gravação.

- Retire

Exclui permanentemente a relação entre a origem e o destino selecionados. Os volumes não são destruídos e as cópias Snapshot nos volumes não são removidas. Esta operação não pode ser desfeita.

- Retomar

Permite transferências agendadas para um relacionamento quiesced. No próximo intervalo de transferência programado, um ponto de verificação de reinício é usado, se existir um.

- Ressincronizar

Permite que você ressincronize um relacionamento anteriormente quebrado.

- Inicializar/atualizar

Permite-lhe efetuar uma transferência de linha de base pela primeira vez numa nova relação de proteção ou efetuar uma atualização manual se a relação já estiver inicializada.

- Ressincronização reversa

Permite restabelecer uma relação de proteção anteriormente quebrada, invertendo a função da origem e destino fazendo da fonte uma cópia do destino original. O conteúdo na origem é substituído pelo conteúdo no destino, e todos os dados mais recentes que os dados na cópia Snapshot comum são excluídos.

- Restaurar

Permite restaurar dados de um volume para outro. Para obter informações, "[Restaurar dados utilizando a página de detalhes de volume / Saúde](#)" consulte .



O botão Restaurar e os botões de operação de relacionamento não estão disponíveis para volumes que estão em relações de proteção síncronas.

- **Ver volumes**

Permite navegar para a visualização Saúde: Todos os volumes.

### **Separador capacidade**

A guia capacidade exibe detalhes sobre o volume selecionado, como sua capacidade física, capacidade lógica, configurações de limite, capacidade de cota e informações sobre qualquer operação de movimentação de volume:

- **Capacidade física**

Detalha a capacidade física do volume:

- Sobrecarga de instantâneos

Exibe o espaço de dados consumido pelas cópias Snapshot.

- Usado

Exibe o espaço usado pelos dados no volume.

- Aviso

Indica que o espaço no volume está quase cheio. Se esse limite for violado, o evento espaço quase cheio será gerado.

- Erro

Indica que o espaço no volume está cheio. Se esse limite for violado, o evento espaço cheio será gerado.

- Inutilizável

Indica que o evento espaço de volume em risco com provisionamento reduzido é gerado e que o espaço no volume provisionado com provisionamento reduzido está em risco devido a problemas de capacidade agregada. A capacidade inutilizável é exibida apenas para volumes provisionados de forma fina.

- Gráfico de dados

Apresenta a capacidade total de dados e a capacidade de dados utilizada do volume.

Se o crescimento automático estiver ativado, o gráfico de dados também exibirá o espaço disponível no agregado. O gráfico de dados exibe o espaço de armazenamento efetivo que pode ser usado pelos dados no volume, que pode ser um dos seguintes:

- Capacidade de dados real do volume para as seguintes condições:
  - O crescimento automático está desativado.
  - O volume ativado para crescimento automático atingiu o tamanho máximo.
  - O volume provisionado thickly habilitado para crescimento automático não pode crescer ainda mais.
- Capacidade de dados do volume depois de considerar o tamanho máximo do volume (para volumes provisionados com pouco provisionamento e para volumes provisionados com thickly quando o agregado tem espaço para que o volume alcance o tamanho máximo)
- Capacidade de dados do volume depois de considerar o próximo tamanho possível com crescimento automático (para volumes provisionados com thickly que têm um limite de porcentagem com crescimento automático)

- Gráfico de cópias Snapshot

Este gráfico é exibido apenas quando a capacidade Snapshot usada ou a reserva Instantânea não é zero.

Ambos os gráficos exibem a capacidade pela qual a capacidade de captura instantânea excede a reserva de captura instantânea se a capacidade de captura instantânea usada exceder a reserva de captura instantânea.

- **Capacidade lógica**

Apresenta as características do espaço lógico do volume. O espaço lógico indica o tamanho real dos dados que estão sendo armazenados em disco sem aplicar a economia com o uso das tecnologias de eficiência de storage da ONTAP.

- Relatórios de espaço lógico



Exibe se o volume tem relatórios de espaço lógico configurados. O valor pode ser ativado, Desativado ou não aplicável. "não aplicável" é exibido para volumes em versões mais antigas do ONTAP ou em volumes que não suportam relatórios de espaço lógico.

- Usado

Exibe a quantidade de espaço lógico que está sendo usado pelos dados no volume e a porcentagem de espaço lógico usado com base na capacidade total de dados.

- Aplicação do espaço lógico

Exibe se a imposição de espaço lógico está configurada para volumes provisionados de forma fina. Quando definido como ativado, o tamanho lógico utilizado do volume não pode ser superior ao tamanho do volume físico atualmente definido.

- **Autowore**

Indica se o volume aumenta automaticamente quando está fora do espaço.

- **Garantia de espaço**

Exibe o controle de configuração FlexVol volume quando um volume remove blocos livres de um agregado. Esses blocos são, então, garantidos para estarem disponíveis para gravações em arquivos no volume. A garantia de espaço pode ser definida para um dos seguintes:

- Nenhum

Nenhuma garantia de espaço está configurada para o volume.

- Ficheiro

É garantido o tamanho completo de ficheiros pouco escritos (por exemplo, LUNs).

- Volume

O tamanho completo do volume é garantido.

- Parcial

O volume FlexCache reserva espaço com base no seu tamanho. Se o tamanho do volume FlexCache for de 100 MB ou mais, a garantia de espaço mínimo será definida como 100 MB por padrão. Se o tamanho do volume FlexCache for inferior a 100 MB, a garantia de espaço mínimo será definida para o tamanho do volume FlexCache. Se o tamanho do volume FlexCache for aumentado mais tarde, a garantia de espaço mínimo não será incrementada.



A garantia de espaço é parcial quando o volume é do tipo Data-Cache.

- **Detalhes (físicos)**

Apresenta as características físicas do volume.

- \* Capacidade total\*

Exibe a capacidade física total no volume.

- **Capacidade de dados**

Exibe a quantidade de espaço físico usado pelo volume (capacidade usada) e a quantidade de espaço físico que ainda está disponível (capacidade livre) no volume. Esses valores também são exibidos como uma porcentagem da capacidade física total.

Quando o evento espaço de volume em risco de provisionamento reduzido é gerado para volumes provisionados de forma fina, a quantidade de espaço usado pelo volume (capacidade usada) e a quantidade de espaço disponível no volume, mas não pode ser usado (capacidade inutilizável) devido a problemas de capacidade agregada é exibida.

- **Reserva Snapshot**

Exibe a quantidade de espaço usada pelas cópias Snapshot (capacidade usada) e a quantidade de espaço disponível para cópias Snapshot (capacidade gratuita) no volume. Esses valores também são exibidos como uma porcentagem da reserva total de instantâneos.

Quando o evento espaço em risco de volume provisionado com thin é gerado para volumes provisionados com thin, a quantidade de espaço usada pelas cópias Snapshot (capacidade usada) e a quantidade de espaço disponível no volume, mas não pode ser usada para fazer cópias Snapshot (capacidade inutilizável) devido a problemas de capacidade agregada, são exibidas.

- **Limiares de volume**

Exibe os seguintes limites de capacidade de volume:

- Limite quase total

Especifica a porcentagem em que um volume está quase cheio.

- Limite máximo

Especifica a porcentagem na qual um volume está cheio.

- **Outros detalhes**

- Tamanho máximo de crescimento automático

Apresenta o tamanho máximo até ao qual o volume pode crescer automaticamente. O valor padrão é 120% do tamanho do volume na criação. Este campo é exibido apenas quando o crescimento automático está ativado para o volume.

- Capacidade comprometida da cota de Qtree

Exibe o espaço reservado nas cotas.

- Capacidade supercomprometida da cota de Qtree

Exibe a quantidade de espaço que pode ser usada antes que o sistema gere o evento de excesso de cota de volume Qtree.

- Reserva fracionária

Controla o tamanho da reserva de substituição. Por padrão, a reserva fracionária é definida como 100, indicando que 100% do espaço reservado necessário é reservado para que os objetos estejam totalmente protegidos para sobrescritas. Se a reserva fracionária for inferior a 100 por cento, o espaço

reservado para todos os arquivos espaço-reservados nesse volume será reduzido à porcentagem da reserva fracionária.

- Taxa de crescimento diária do Snapshot

Exibe a alteração (em porcentagem ou em KB, MB, GB, etc.) que ocorre a cada 24 horas nas cópias Snapshot no volume selecionado.

- Snapshot dias para cheio

Exibe o número estimado de dias restantes antes que o espaço reservado para as cópias Snapshot no volume atinja o limite especificado.

O campo Snapshot Days to Full (dias instantâneos a cheio) exibe um valor não aplicável quando a taxa de crescimento das cópias Snapshot no volume é zero ou negativa, ou quando não há dados suficientes para calcular a taxa de crescimento.

- Snapshot Autodelete

Especifica se as cópias Snapshot são automaticamente excluídas para liberar espaço quando uma gravação em um volume falha devido à falta de espaço no agregado.

- Cópias Snapshot

Exibe informações sobre as cópias Snapshot no volume.

O número de cópias Snapshot no volume é exibido como um link. Clicar no link abre a caixa de diálogo cópias Snapshot em um volume, que exibe detalhes das cópias Snapshot.

A contagem de cópias snapshot é atualizada aproximadamente a cada hora. No entanto, a lista de cópias snapshot é atualizada no momento em que você clica no ícone. Isso pode resultar em uma diferença entre a contagem de cópias Snapshot exibida na topologia e o número de cópias snapshot listadas quando você clica no ícone.

- **Movimentação de volume**

Exibe o status da operação de movimentação de volume atual ou da última que foi realizada no volume e outros detalhes, como a fase atual da operação de movimentação de volume que está em andamento, agregado de origem, agregado de destino, hora de início, hora de término e hora de término estimada.

Também apresenta o número de operações de movimentação de volume que são executadas no volume selecionado. Você pode ver mais informações sobre as operações de movimentação de volume clicando no link **Histórico de movimentação de volume**.

### **Separador Configuration (Configuração)**

A guia Configuração exibe detalhes sobre o volume selecionado, como política de exportação, tipo RAID, capacidade e recursos relacionados à eficiência de armazenamento do volume:

- **Visão geral**

- Nome completo

Exibe o nome completo do volume.

- Agregados

Exibe o nome do agregado no qual o volume reside ou o número de agregados nos quais o volume FlexGroup reside.

- Política de disposição em camadas

Exibe a política de disposição em camadas definida para o volume; se o volume for implantado em um agregado habilitado para FabricPool. A política pode ser nenhum, somente Snapshot, Backup, Automático ou tudo.

- Armazenamento VM

Exibe o nome do SVM que contém o volume.

- Caminho de junção

Exibe o status do caminho, que pode estar ativo ou inativo. O caminho no SVM no qual o volume é montado também é exibido. Você pode clicar no link **Histórico** para ver as cinco alterações mais recentes no caminho de junção.

- Política de exportação

Exibe o nome da política de exportação criada para o volume. Você pode clicar no link para exibir detalhes sobre as políticas de exportação, protocolos de autenticação e acesso habilitados nos volumes que pertencem ao SVM.

- Estilo

Apresenta o estilo do volume. O estilo de volume pode ser FlexVol ou FlexGroup.

- Tipo

Apresenta o tipo do volume selecionado. O tipo de volume pode ser leitura-escrita, compartilhamento de carga, proteção de dados, cache de dados ou temporário.

- Tipo RAID

Exibe o tipo RAID do volume selecionado. O tipo RAID pode ser RAID0, RAID4, RAID-DP ou RAID-TEC.



Vários tipos de RAID podem ser exibidos para volumes FlexGroup porque os volumes constituintes para FlexGroups podem estar em agregados de diferentes tipos.

- Tipo SnapLock

Exibe o tipo de SnapLock do agregado que contém o volume.

- Expiração do SnapLock

Apresenta a data de validade do volume SnapLock.

- **Capacidade**

- Thin Provisioning

Exibe se o provisionamento de thin está configurado para o volume.

- Crescimento automático

Exibe se o volume flexível cresce automaticamente dentro de um agregado.

- Snapshot Autodelete

Especifica se as cópias Snapshot são automaticamente excluídas para liberar espaço quando uma gravação em um volume falha devido à falta de espaço no agregado.

- Quotas

Especifica se as cotas estão ativadas para o volume.

#### • **Eficiência**

- Compactação

Especifica se a compressão está ativada ou desativada.

- Deduplicação

Especifica se a deduplicação está ativada ou desativada.

- Modo de deduplicação

Especifica se a operação de deduplicação ativada em um volume é uma operação manual, agendada ou baseada em políticas. Se o modo estiver definido como programado, o agendamento de operação será exibido e, se o modo estiver definido como uma política, o nome da política será exibido.

- Tipo de deduplicação

Especifica o tipo de operação de deduplicação em execução no volume. Se o volume estiver em uma relação SnapVault, o tipo exibido será SnapVault. Para qualquer outro volume, o tipo é exibido como regular.

- Política de eficiência de storage

Especifica o nome da política de eficiência de storage atribuída pelo Unified Manager a esse volume. Essa política pode controlar as configurações de compactação e deduplicação.

#### • **Proteção**

- Cópias Snapshot

Especifica se as cópias Snapshot automáticas estão ativadas ou desativadas.

#### **Patilha de proteção**

A guia proteção exibe detalhes de proteção sobre o volume selecionado, como informações de atraso, tipo de relacionamento e topologia da relação.

#### • **Resumo**

Exibe as propriedades de relacionamentos de proteção (SnapMirror, SnapVault ou Storage VM DR) para um volume selecionado. Para qualquer outro tipo de relacionamento, somente a propriedade tipo de

relacionamento é exibida. Se um volume primário for selecionado, somente a Diretiva de cópia Snapshot gerenciada e local será exibida. As propriedades exibidas para relacionamentos SnapMirror e SnapVault incluem o seguinte:

- Volume de origem

Apresenta o nome da fonte do volume selecionado se o volume selecionado for um destino.

- Estado de atraso

Exibe o status de atraso de atualização ou transferência para uma relação de proteção. O status pode ser erro, Aviso ou crítico.

O status de atraso não é aplicável para relacionamentos síncronos.

- Duração do atraso

Apresenta a hora pela qual os dados no espelho ficam atrás da fonte.

- Última atualização bem-sucedida

Exibe a data e a hora da atualização de proteção bem-sucedida mais recente.

A última atualização bem-sucedida não se aplica a relacionamentos síncronos.

- Membro do Serviço de armazenamento

Exibe Sim ou não para indicar se o volume pertence ou não e é gerenciado por um serviço de armazenamento.

- Versão flexível replicação

Exibe Sim, Sim com a opção de backup ou nenhum. Sim indica que a replicação do SnapMirror é possível mesmo que os volumes de origem e destino estejam executando versões diferentes do software ONTAP. Sim com a opção de backup indica a implementação da proteção SnapMirror com a capacidade de reter várias versões de cópias de backup no destino. Nenhum indica que a replicação flexível da versão não está ativada.

- Capacidade de relacionamento

Indica os recursos do ONTAP disponíveis para o relacionamento de proteção.

- Serviço de proteção

Exibe o nome do serviço de proteção se o relacionamento for gerenciado por um aplicativo do parceiro de proteção.

- Tipo de relacionamento

Exibe qualquer tipo de relacionamento, incluindo espelhamento assíncrono, cofre assíncrono, espelhamento assíncrono, StrictSync e sincronização.

- Estado relação

Exibe o estado da relação SnapMirror ou SnapVault. O estado pode ser não inicializado, SnapMirrored ou quebrado. Se for selecionado um volume de origem, o estado da relação não é aplicável e não é

apresentado.

- Estado da transferência

Exibe o status da transferência para a relação de proteção. O estado da transferência pode ser um dos seguintes:

- A abortar

As transferências SnapMirror estão ativadas; no entanto, uma operação de cancelamento de transferência que pode incluir a remoção do ponto de verificação está em andamento.

- Verificação

O volume de destino está passando por uma verificação de diagnóstico e nenhuma transferência está em andamento.

- A finalizar

As transferências SnapMirror estão ativadas. O volume está atualmente na fase pós-transferência para transferências incrementais de SnapVault.

- Ocioso

As transferências estão ativadas e nenhuma transferência está em curso.

- Sincronização in-Sync

Os dados nos dois volumes na relação síncrona são sincronizados.

- Fora de sincronização

Os dados no volume de destino não são sincronizados com o volume de origem.

- Preparar

As transferências SnapMirror estão ativadas. O volume está atualmente na fase de pré-transferência para transferências incrementais de SnapVault.

- Em fila de espera

As transferências SnapMirror estão ativadas. Nenhuma transferência está em andamento.

- Quiesced

As transferências SnapMirror estão desativadas. Nenhuma transferência está em andamento.

- Quiescing

Uma transferência SnapMirror está em andamento. As transferências adicionais estão desativadas.

- A transferir

As transferências SnapMirror estão ativadas e uma transferência está em curso.

- Em transição

A transferência assíncrona de dados da origem para o volume de destino está concluída e a transição para a operação síncrona foi iniciada.

- A aguardar

Uma transferência SnapMirror foi iniciada, mas algumas tarefas associadas estão aguardando para serem enfileiradas.

- Taxa de transferência máxima

Apresenta a taxa de transferência máxima para a relação. A taxa de transferência máxima pode ser um valor numérico em kilobytes por segundo (Kbps), megabytes por segundo (Mbps), Gigabytes por segundo (Gbps) ou Terabytes por segundo (Tbps). Se não for exibido nenhum limite, a transferência de linha de base entre relacionamentos é ilimitada.

- Política de SnapMirror

Exibe a política de proteção do volume. DPDefault indica a política de proteção de espelho assíncrono padrão, XDPDefault indica a política de cofre assíncrono padrão e DPSyncDefault indica a política de espelhamento assíncrono padrão. StrictSync indica a política de proteção estrita síncrona padrão e Sync indica a política síncrona padrão. Você pode clicar no nome da política para exibir detalhes associados a essa política, incluindo as seguintes informações:

- Prioridade de transferência
- Ignorar a definição de hora de acesso
- Limite de tentativas
- Comentários
- Etiquetas SnapMirror
- Definições de retenção
- Cópias Snapshot reais
- Preservar cópias Snapshot
- Limite de aviso de retenção
- Cópias snapshot sem configurações de retenção em uma relação de SnapVault em cascata onde a origem é um volume de proteção de dados (DP), apenas a regra "m\_created" se aplica.

- Atualizar Programa

Exibe a programação SnapMirror atribuída à relação. Posicionar o cursor sobre o ícone de informações exibe os detalhes da programação.

- Política de instantâneo local

Exibe a política de cópia Snapshot do volume. A política é padrão, nenhum ou qualquer nome dado a uma política personalizada.

- Protegido por

Apresenta o tipo de proteção utilizado para o volume selecionado. Por exemplo, se um volume estiver protegido pelas relações de grupo de consistência e volume SnapMirror, este campo exibirá SnapMirror e Grupo de consistência. Esse campo também fornece um link que redireciona você para a



página relacionamentos para exibir o status do relacionamento unificado. O link só é aplicável às relações constituintes.

- Grupo de consistência

Para volumes protegidos pelas relações de sincronização ativa do SnapMirror, esta coluna exibe o Grupo de consistência do volume.

## • Vistas

Exibe a topologia de proteção do volume selecionado. A topologia inclui representações gráficas de todos os volumes relacionados ao volume selecionado. O volume selecionado é indicado por uma borda cinza escura e as linhas entre os volumes na topologia indicam o tipo de relação de proteção. A direção das relações na topologia é exibida da esquerda para a direita, com a origem de cada relação à esquerda e o destino à direita.

Linhas em negrito duplas especificam uma relação de espelhamento assíncrono, uma única linha em negrito especifica uma relação de cofre assíncrono, linhas únicas duplas especificam uma relação de espelhamento assíncrono e uma linha em negrito e não negrito especificam uma relação síncrona. A tabela abaixo indica se a relação síncrona é StrictSync ou Sync.

Clicar com o botão direito do Mouse em um volume exibe um menu do qual você pode escolher para proteger o volume ou restaurar dados para ele. Clicar com o botão direito do Mouse em uma relação exibe um menu no qual você pode escolher editar, abortar, quiesce, quebrar, remover ou retomar uma relação.

Os menus não serão exibidos nas seguintes instâncias:

- Se as configurações RBAC não permitirem essa ação, por exemplo, se você tiver apenas Privileges de operador
- Se o volume estiver em uma relação de proteção síncrona
- Quando o ID do volume é desconhecido, por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto clicando em outro volume na topologia seleciona e exibe informações para esse volume. Um ponto de interrogação ( ? ) no canto superior esquerdo de um volume indica que o volume está ausente ou que ainda não foi descoberto. Ele também pode indicar que as informações de capacidade estão ausentes. Posicionar o cursor sobre o ponto de interrogação exibe informações adicionais, incluindo sugestões para ações corretivas.

A topologia exibe informações sobre capacidade de volume, atraso, cópias Snapshot e última transferência de dados bem-sucedida se estiver em conformidade com um dos vários modelos de topologia comuns. Se uma topologia não estiver em conformidade com um desses modelos, as informações sobre o atraso de volume e a última transferência de dados bem-sucedida serão exibidas em uma tabela de relacionamento sob a topologia. Nesse caso, a linha realçada na tabela indica o volume selecionado e, na vista de topologia, as linhas a negrito com um ponto azul indicam a relação entre o volume selecionado e o volume de origem.

As visualizações de topologia incluem as seguintes informações:


## • Capacidade

Apresenta a quantidade total de capacidade utilizada pelo volume. Posicionar o cursor sobre um volume na topologia exibe as configurações atuais de aviso e limite crítico para esse volume na caixa de diálogo Configurações de limite atuais. Você também pode editar as configurações de limite clicando no link **Editar limites** na caixa de diálogo Configurações de limite atuais. A caixa de seleção **Capacity** oculta todas as informações de capacidade de todos os volumes na topologia.

- Atraso

Exibe a duração do atraso e o status do atraso das relações de proteção recebidas. Desmarcar a caixa de seleção **lag** oculta todas as informações de lag para todos os volumes na topologia. Quando a caixa de seleção **lag** está esmaecida, as informações de lag para o volume selecionado são exibidas na tabela de relacionamento abaixo da topologia, bem como as informações de lag para todos os volumes relacionados.

- Snapshot

Exibe o número de cópias Snapshot disponíveis para um volume. Desmarcar a caixa de seleção **Snapshot** oculta todas as informações de cópia Snapshot para todos os volumes na topologia. Clicar em um ícone de cópia Snapshot (  ) exibe a lista cópia Snapshot de um volume. A contagem de cópias snapshot exibida ao lado do ícone é atualizada aproximadamente a cada hora. No entanto, a lista de cópias snapshot é atualizada no momento em que você clica no ícone. Isso pode resultar em uma diferença entre a contagem de cópias Snapshot exibida na topologia e o número de cópias snapshot listadas quando você clica no ícone.

- Última transferência bem-sucedida

Exibe a quantidade, a duração, a hora e a data da última transferência de dados bem-sucedida. Quando a caixa de verificação **Last successful Transfer** (última transferência bem-sucedida) estiver esmaecida, as últimas informações de transferência bem-sucedidas para o volume selecionado são exibidas na tabela de relacionamento abaixo da topologia, bem como as últimas informações de transferência bem-sucedidas para todos os volumes relacionados.

- **História**

Exibe em um gráfico o histórico das relações de proteção SnapMirror e SnapVault recebidas para o volume selecionado. Existem três gráficos de histórico disponíveis: Duração do atraso de relacionamento de entrada, duração da transferência de relacionamento de entrada e tamanho da transferência de relacionamento de entrada. As informações do histórico são exibidas somente quando você seleciona um volume de destino. Se selecionar um volume primário, os gráficos ficam vazios e é apresentada a mensagem no data found (sem dados encontrados). Se os volumes estiverem protegidos pelas relações síncronas do Grupo de consistência e do SnapMirror, as informações sobre a duração da transferência de relacionamento e o tamanho da transferência de relacionamento não serão exibidas.

Você pode selecionar um tipo de gráfico na lista suspensa na parte superior do painel Histórico. Você também pode exibir detalhes de um período de tempo específico selecionando 1 semana, 1 mês ou 1 ano. Gráficos de histórico podem ajudá-lo a identificar tendências: Por exemplo, se grandes quantidades de dados estão sendo transferidos ao mesmo tempo do dia ou da semana, ou se o aviso de atraso ou o limite de erro de atraso está sendo violado consistentemente, você pode tomar a ação apropriada. Além disso, você pode clicar no botão **Exportar** para criar um relatório em formato CSV para o gráfico que você está visualizando.

Os gráficos do histórico de proteção apresentam as seguintes informações:

- **Duração do atraso do relacionamento**

Exibe segundos, minutos ou horas no eixo vertical (y) e exibe dias, meses ou anos no eixo horizontal (x), dependendo do período de duração selecionado. O valor superior no eixo y indica a duração máxima de atraso alcançada no período de duração mostrado no eixo x. A linha laranja horizontal no gráfico representa o limiar de erro de atraso e a linha amarela horizontal representa o limiar de aviso de atraso.

Posicionar o cursor sobre estas linhas apresenta a definição de limiar. A linha azul horizontal representa a duração do atraso. Você pode visualizar os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área de interesse.

- **Duração da transferência de relacionamento**

Exibe segundos, minutos ou horas no eixo vertical (y) e exibe dias, meses ou anos no eixo horizontal (x), dependendo do período de duração selecionado. O valor superior no eixo y indica a duração máxima de transferência alcançada no período de duração mostrado no eixo x. Você pode visualizar os detalhes de pontos específicos no gráfico posicionando o cursor sobre a área de interesse.



Esse gráfico não está disponível para volumes que estão em relacionamentos de proteção síncronos.

- \* Tamanho transferido da relação\*

Exibe bytes, kilobytes, megabytes, etc., no eixo vertical (y), dependendo do tamanho da transferência, e exibe dias, meses ou anos no eixo horizontal (x), dependendo do período de tempo selecionado. O valor superior no eixo y indica o tamanho máximo de transferência atingido no período de duração mostrado no eixo x. Você pode visualizar os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área de interesse.



Esse gráfico não está disponível para volumes que estão em relacionamentos de proteção síncronos.

## Área de história

A área Histórico exibe gráficos que fornecem informações sobre a capacidade e as reservas de espaço do volume selecionado. Além disso, você pode clicar no botão **Exportar** para criar um relatório em formato CSV para o gráfico que você está visualizando.

Os gráficos podem estar vazios e a mensagem nenhum dado encontrado é exibida quando os dados ou o estado do volume permanecem inalterados por um período de tempo.

Você pode selecionar um tipo de gráfico na lista suspensa na parte superior do painel Histórico. Você também pode exibir detalhes de um período de tempo específico selecionando 1 semana, 1 mês ou 1 ano. Gráficos de histórico podem ajudá-lo a identificar tendências - por exemplo, se o uso de volume estiver constantemente violando o limite quase completo, você pode tomar a ação apropriada.

Os gráficos de histórico apresentam as seguintes informações:

- **Capacidade de volume utilizada**

Exibe a capacidade usada no volume e a tendência em como a capacidade do volume é usada com base no histórico de uso, como gráficos de linha em bytes, kilobytes, megabytes, e assim por diante, no eixo vertical (y). O período de tempo é apresentado no eixo horizontal (x). Você pode selecionar um período de tempo de uma semana, um mês ou um ano. Você pode exibir os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linha clicando na legenda apropriada. Por exemplo, quando você clica na legenda volume usado capacidade, a linha do gráfico volume usado capacidade é oculta.

- **Capacidade de volume utilizada vs total**

Exibe a tendência de como a capacidade de volume é usada com base no histórico de uso, bem como a

capacidade usada, capacidade total e detalhes da economia de espaço da deduplicação e compactação, como gráficos de linha, em bytes, kilobytes, megabytes, e assim por diante, no eixo vertical (y). O período de tempo é apresentado no eixo horizontal (x). Você pode selecionar um período de tempo de uma semana, um mês ou um ano. Você pode exibir os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linha clicando na legenda apropriada. Por exemplo, quando você clica na legenda capacidade de tendência usada, a linha de gráfico capacidade de tendência usada fica oculta.

- **Capacidade de volume utilizada (%)**

Exibe a capacidade usada no volume e a tendência de como a capacidade do volume é usada com base no histórico de uso, como gráficos de linha, em porcentagem, no eixo vertical (y). O período de tempo é apresentado no eixo horizontal (x). Você pode selecionar um período de tempo de uma semana, um mês ou um ano. Você pode exibir os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linha clicando na legenda apropriada. Por exemplo, quando você clica na legenda volume usado capacidade, a linha do gráfico volume usado capacidade é oculta.

- **Capacidade do instantâneo usada (%)**

Exibe o limite de aviso de reserva instantânea e instantâneo como gráficos de linha e a capacidade usada pelas cópias Snapshot como um gráfico de área, em porcentagem, no eixo vertical (y). O estouro instantâneo é representado com cores diferentes. O período de tempo é apresentado no eixo horizontal (x). Você pode selecionar um período de tempo de uma semana, um mês ou um ano. Você pode exibir os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linha clicando na legenda apropriada. Por exemplo, quando você clica na legenda reserva Instantânea, a linha do gráfico reserva Instantânea fica oculta.

#### **Lista de eventos**

A lista Eventos exibe detalhes sobre eventos novos e reconhecidos:

- **Gravidade**

Exibe a gravidade do evento.

- **Evento**

Exibe o nome do evento.

- **Tempo acionado**

Exibe o tempo decorrido desde que o evento foi gerado. Se o tempo decorrido exceder uma semana, o carimbo de data/hora quando o evento foi gerado é exibido.

#### **Painel Anotações relacionadas**

O painel Anotações relacionadas permite-lhe visualizar detalhes da anotação associados ao volume selecionado. Os detalhes incluem o nome da anotação e os valores da anotação que são aplicados ao volume. Também pode remover anotações manuais do painel Anotações relacionadas.

#### **Painel dispositivos relacionados**

O painel dispositivos relacionados permite exibir e navegar para SVMs, agregados, qtrees, LUNs e cópias Snapshot relacionadas ao volume:

- **Storage Virtual Machine**

Exibe a capacidade e o status de integridade do SVM que contém o volume selecionado.

- **Agregado**

Exibe a capacidade e o status de integridade do agregado que contém o volume selecionado. Para volumes FlexGroup, o número de agregados que compõem o FlexGroup é listado.

- **Volumes no agregado**

Exibe o número e a capacidade de todos os volumes que pertencem ao agregado pai do volume selecionado. O estado de funcionamento dos volumes também é apresentado, com base no nível de gravidade mais elevado. Por exemplo, se um agregado contiver dez volumes, cinco dos quais exibem o status de Aviso e os cinco restantes exibem o status crítico, o status exibido será crítico. Este componente não aparece para volumes FlexGroup.

- **Qtrees**

Exibe o número de qtrees que o volume selecionado contém e a capacidade de qtrees com cota que o volume selecionado contém. A capacidade dos qtrees com cota é exibida em relação à capacidade de dados de volume. O estado de saúde do qtrees também é exibido, com base no nível de gravidade mais alto. Por exemplo, se um volume tiver dez qtrees, cinco com status de Aviso e os cinco restantes com status crítico, o status exibido será crítico.

- **Compartilhamentos NFS**

Exibe o número e o status dos compartilhamentos NFS associados ao volume.

- **Compartilhamentos SMB**

Exibe o número e o status dos compartilhamentos SMB/CIFS.

- **LUNs**

Exibe o número e o tamanho total de todos os LUNs no volume selecionado. O estado de funcionamento dos LUNs também é apresentado, com base no nível de gravidade mais elevado.

- **Cotas de usuários e grupos**

Exibe o número e o status das cotas de usuário e grupo de usuários associadas ao volume e suas qtrees.

- **Volumes FlexClone**

Exibe o número e a capacidade de todos os volumes clonados do volume selecionado. O número e a capacidade são apresentados apenas se o volume selecionado contiver quaisquer volumes clonados.

- **Volume principal**

Exibe o nome e a capacidade do volume pai de um volume FlexClone selecionado. O volume principal é exibido somente se o volume selecionado for um volume FlexClone.

#### **Painel grupos relacionados**

O painel grupos relacionados permite exibir a lista de grupos associados ao volume selecionado.

## Painel Alertas relacionados

O painel Alertas relacionados permite visualizar a lista de alertas criados para o volume selecionado. Você também pode adicionar um alerta clicando no link Adicionar alerta ou editar um alerta existente clicando no nome do alerta.

## Página de detalhes de VM/integridade de armazenamento

Você pode usar a página de detalhes de integridade/VM de armazenamento para exibir informações detalhadas sobre a VM de armazenamento selecionada, como integridade, capacidade, configuração, políticas de dados, interfaces lógicas (LIFs), LUNs, qtrees, usuário, cotas de grupo de usuários e detalhes de proteção. Você também pode exibir informações sobre os objetos relacionados e alertas relacionados para a VM de storage.



Você só pode monitorar VM de storage de dados.

## Botões de comando

Os botões de comando permitem executar as seguintes tarefas para a VM de armazenamento selecionada:

- **Mude para a visualização de desempenho**

Permite navegar para a página de detalhes de VM/desempenho de armazenamento.

- **Ações**

- Adicionar alerta

Permite adicionar um alerta à VM de armazenamento selecionada.

- Anotar

Permite anotar a VM de armazenamento selecionada.

- **Exibir VMs de armazenamento**

Permite navegar para a visualização integridade: Todas as VMs de armazenamento.

## Separador Saúde

A guia integridade exibe informações detalhadas sobre disponibilidade, capacidade e problemas de proteção de dados de vários objetos, como volumes, agregados, LIFs nas, LIFs SAN, LUNs, protocolos, serviços, compartilhamentos NFS e compartilhamentos CIFS.

Você pode clicar no gráfico de um objeto para exibir a lista filtrada de objetos. Por exemplo, você pode clicar no gráfico de capacidade de volume que exibe avisos para exibir a lista de volumes que têm problemas de capacidade com gravidade como aviso.

- **Problemas de disponibilidade**

Exibe, como um gráfico, o número total de objetos, incluindo objetos que têm problemas de disponibilidade e objetos que não têm problemas relacionados à disponibilidade. As cores no gráfico representam os diferentes níveis de gravidade dos problemas. As informações abaixo do gráfico fornecem detalhes sobre problemas de disponibilidade que podem afetar ou que já afetaram a disponibilidade de

dados na VM de armazenamento. Por exemplo, são exibidas informações sobre os LIFs nas e os LIFs SAN inativos e volumes offline.

Você também pode exibir informações sobre os protocolos e serviços relacionados que estão sendo executados no momento, bem como o número e o status dos compartilhamentos NFS e CIFS.

- **Problemas de capacidade**

Exibe, como um gráfico, o número total de objetos, incluindo objetos que têm problemas de capacidade e objetos que não têm problemas relacionados à capacidade. As cores no gráfico representam os diferentes níveis de gravidade dos problemas. As informações abaixo do gráfico fornecem detalhes sobre problemas de capacidade que podem afetar ou que já afetaram a capacidade dos dados na VM de armazenamento. Por exemplo, informações são exibidas sobre agregados que provavelmente violarão os valores de limite definidos.

- \* Questões de proteção\*

Fornecer uma visão geral rápida da integridade relacionada à proteção da VM de storage exibindo, como uma caixa de diálogo de campo, o número total de relacionamentos, incluindo relacionamentos que têm problemas de proteção e relacionamentos que não têm problemas relacionados à proteção. Você também pode exibir o status da relação de recuperação de desastres da VM de storage selecionada. Os eventos de relacionamentos de DR de VM de storage são exibidos aqui e clicar nos eventos leva você à página de detalhes do evento. Quando existem volumes desprotegidos, clicar no link leva você para a exibição integridade: Todos os volumes, onde você pode exibir uma lista filtrada dos volumes desprotegidos na VM de armazenamento. As cores no gráfico representam os diferentes níveis de gravidade dos problemas. Clicar em um gráfico leva você para a exibição relacionamento: Todos os relacionamentos, onde você pode exibir uma lista filtrada de detalhes da relação de proteção. As informações abaixo do gráfico fornecem detalhes sobre problemas de proteção que podem afetar ou que já afetaram a proteção de dados na VM de armazenamento. Por exemplo, são exibidas informações sobre volumes que têm uma reserva de cópia Snapshot quase cheia ou sobre problemas de atraso de relacionamento com o SnapMirror.

## **Separador capacidade**

A guia capacidade exibe informações detalhadas sobre a capacidade de dados do SVM selecionado.

As seguintes informações são exibidas para uma VM de armazenamento com volume FlexVol volume ou FlexGroup:

- **Capacidade**

A área capacidade exibe detalhes sobre a capacidade usada e disponível alocada de todos os volumes:

- Capacidade total

Exibe a capacidade total da VM de armazenamento.

- Usado

Exibe o espaço usado pelos dados nos volumes que pertencem à VM Storage.

- Garantido disponível

Exibe o espaço disponível garantido para os dados disponíveis para volumes na VM Storage.

- Sem garantia

Exibe o espaço disponível restante para os dados alocados para volumes provisionados com precisão na VM de armazenamento.

- **Volumes com problemas de capacidade**

A lista volumes com problemas de capacidade exibe, em formato tabular, detalhes sobre os volumes com problemas de capacidade:

- Estado

Indica que o volume tem um problema relacionado com a capacidade de uma gravidade indicada.

Você pode mover o ponteiro sobre o status para exibir mais informações sobre o evento relacionado à capacidade ou eventos gerados para o volume.

Se o status do volume for determinado por um único evento, você poderá exibir informações como o nome do evento, a hora e a data em que o evento foi acionado, o nome do administrador a quem o evento foi atribuído e a causa do evento. Você pode usar o botão **Exibir detalhes** para ver mais informações sobre o evento.

Se o status do volume for determinado por vários eventos da mesma gravidade, os três principais eventos serão exibidos com informações como o nome do evento, a hora e a data em que os eventos foram acionados e o nome do administrador ao qual o evento foi atribuído. Você pode ver mais detalhes sobre cada um desses eventos clicando no nome do evento. Você também pode clicar no link **Exibir todos os eventos** para visualizar a lista de eventos gerados.



Um volume pode ter vários eventos da mesma gravidade ou severidades diferentes. No entanto, apenas a gravidade mais alta é exibida. Por exemplo, se um volume tiver dois eventos com severidades de erro e aviso, somente a gravidade do erro será exibida.

- Volume

Exibe o nome do volume.

- Capacidade de dados utilizada

Exibe, como um gráfico, informações sobre o uso da capacidade de volume (em porcentagem).

- Dias para cheio

Apresenta o número estimado de dias restantes antes de o volume atingir a capacidade total.

- Thin Provisioning

Indica se a garantia de espaço está definida para o volume selecionado. Os valores válidos são Sim e não

- Agregados

Para volumes FlexVol, exibe o nome do agregado que contém o volume. Para volumes FlexGroup, exibe o número de agregados que são usados no FlexGroup.



## Separador Configuration (Configuração)

A guia Configuração exibe detalhes de configuração sobre a VM de armazenamento selecionada, como o cluster, o volume raiz, o tipo de volumes que ela contém (volumes FlexVol), políticas e proteção criados na VM de armazenamento:

### • Visão geral

#### ◦ Cluster

Exibe o nome do cluster ao qual a VM de armazenamento pertence.

#### ◦ Tipo de volume permitido

Exibe o tipo de volumes que podem ser criados na VM de armazenamento. O tipo pode ser FlexVol ou FlexVol/FlexGroup.

#### ◦ Volume raiz

Exibe o nome do volume raiz da VM de armazenamento.

#### ◦ Protocolos permitidos

Exibe o tipo de protocolos que podem ser configurados na VM de armazenamento. Indica também se um protocolo está para cima (●), para baixo (●) ou não está configurado (●).

### • \* Interfaces de rede de dados\*

#### ◦ NAS

Exibe o número de interfaces nas associadas à VM de storage. Indica também se as interfaces estão para cima (●) ou para baixo (●).

#### ◦ SAN

Exibe o número de interfaces SAN associadas à VM de storage. Indica também se as interfaces estão para cima (●) ou para baixo (●).

#### ◦ FC-NVMe

Exibe o número de interfaces FC-NVMe associadas à VM de storage. Indica também se as interfaces estão para cima (●) ou para baixo (●).

### • \* Gestão de interfaces de rede\*

#### ◦ Disponibilidade

Exibe o número de interfaces de gerenciamento associadas à VM de storage. Indica também se as interfaces de gestão estão para cima (●) ou para baixo (●).

### • Políticas

#### ◦ Instantâneos

Exibe o nome da política Snapshot criada na VM Storage.

#### ◦ Políticas de exportação

Exibe o nome da política de exportação se uma única política for criada ou exibe o número de políticas de exportação se várias políticas forem criadas.

- **Proteção**

- Storage VM DR

Exibe se a VM de storage selecionada está protegida, destino ou desprotegida e o nome do destino no qual a VM de storage está protegida. Se a VM de armazenamento selecionada for o destino, os detalhes da VM de armazenamento de origem serão exibidos. No caso de fan-out, este campo exibe o número total de VMs de armazenamento de destino nas quais a VM de armazenamento está protegida. O link contagem leva você à grade de relacionamento de VM de armazenamento filtrada na VM de armazenamento de origem.

- Volumes protegidos

Exibe o número de volumes protegidos na VM de armazenamento selecionada do total de volumes. Se você estiver exibindo uma VM de armazenamento de destino, o link número será para os volumes de destino da VM de armazenamento selecionada.

- Volumes não protegidos

Exibe o número de volumes desprotegidos na VM de storage selecionada.

- **Serviços**

- Tipo

Exibe o tipo de serviço configurado na VM de armazenamento. O tipo pode ser Domain Name System (DNS) ou Network Information Service (NIS).

- Estado

Exibe o estado do serviço, que pode ser para cima (●), para baixo (●) ou não configurado (●).

- Nome de domínio

Exibe os nomes de domínio totalmente qualificados (FQDNs) do servidor DNS para os serviços DNS ou servidor NIS para os serviços NIS. Quando o servidor NIS está ativado, o FQDN ativo do servidor NIS é exibido. Quando o servidor NIS está desativado, a lista de todos os FQDNs é exibida.

- Endereço IP

Exibe os endereços IP do servidor DNS ou NIS. Quando o servidor NIS está ativado, é apresentado o endereço IP ativo do servidor NIS. Quando o servidor NIS está desativado, é apresentada a lista de todos os endereços IP.

### **Separador interfaces de rede**

A guia interfaces de rede exibe detalhes sobre as interfaces de rede de dados (LIFs) criadas na VM de armazenamento selecionada:

- **Interface de rede**

Exibe o nome da interface criada na VM de armazenamento selecionada.

- **Status operacional**

Exibe o status operacional da interface, que pode ser para cima (↑), para baixo (↓) ou desconhecido (?). O status operacional de uma interface é determinado pelo status de suas portas físicas.

- **Estado Administrativo**

Exibe o status administrativo da interface, que pode ser para cima (↑), para baixo (↓) ou desconhecido (?). O status administrativo de uma interface é controlado pelo administrador de armazenamento para fazer alterações na configuração ou para fins de manutenção. O estado administrativo pode ser diferente do estado operacional. No entanto, se o status administrativo de uma interface estiver inativo, o status operacional será desativado por padrão.

- \* Endereço IP / WWPN\*

Exibe o endereço IP das interfaces Ethernet e o World Wide Port Name (WWPN) para FC LIFs.

- **Protocolos**

Exibe a lista de protocolos de dados especificados para a interface, como CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe e FlexCache.

- **Função**

Exibe a função de interface. As funções podem ser dados ou Gerenciamento.

- **Porto de casa**

Exibe a porta física à qual a interface foi originalmente associada.

- **Porta atual**

Exibe a porta física à qual a interface está atualmente associada. Se a interface for migrada, a porta atual pode ser diferente da porta inicial.

- **Conjunto de portas**

Exibe o conjunto de portas para o qual a interface é mapeada.

- **Política de failover**

Exibe a política de failover configurada para a interface. Para interfaces NFS, CIFS e FlexCache, a política de failover padrão é Next Available. A política de failover não se aplica a interfaces FC e iSCSI.

- **Grupos de Roteamento**

Exibe o nome do grupo de roteamento. Você pode exibir mais informações sobre as rotas e o gateway de destino clicando no nome do grupo de roteamento.

Os grupos de roteamento não são compatíveis com o ONTAP 8,3 ou posterior e, portanto, uma coluna em branco é exibida para esses clusters.

- **Grupo de failover**

Exibe o nome do grupo de failover.

## Separador Qtrees

A guia Qtrees exibe detalhes sobre qtrees e suas cotas. Você pode clicar no botão **Editar limites** se quiser editar as configurações de limite de integridade para a capacidade de qtree para um ou mais qtrees.

Use o botão **Export** para criar um arquivo de valores separados por vírgulas (.csv) contendo os detalhes de todos os qtrees monitorados. Ao exportar para um arquivo CSV, você pode optar por criar um relatório qtrees para a VM de armazenamento atual, para todas as VMs de armazenamento no cluster atual ou para todas as VMs de armazenamento de todos os clusters no data center. Alguns campos qtrees adicionais aparecem no arquivo CSV exportado.

- **Status**

Exibe o status atual da qtree. O status pode ser crítico (❌), erro (⚠️), Aviso (⚠️) ou normal (✅).

Você pode mover o ponteiro sobre o ícone de status para exibir mais informações sobre o evento ou eventos gerados para a qtree.

Se o status da qtree for determinado por um único evento, você poderá exibir informações como o nome do evento, a hora e a data em que o evento foi acionado, o nome do administrador a quem o evento foi atribuído e a causa do evento. Você pode usar **Exibir detalhes** para ver mais informações sobre o evento.

Se o status da qtree for determinado por vários eventos da mesma gravidade, os três principais eventos serão exibidos com informações como o nome do evento, a hora e a data em que os eventos foram acionados e o nome do administrador ao qual o evento foi atribuído. Você pode ver mais detalhes sobre cada um desses eventos clicando no nome do evento. Você também pode usar **Exibir todos os eventos** para visualizar a lista de eventos gerados.



Uma qtree pode ter vários eventos da mesma gravidade ou gravidades diferentes. No entanto, apenas a gravidade mais alta é exibida. Por exemplo, se uma qtree tiver dois eventos com severidades de erro e aviso, somente a gravidade do erro será exibida.

- **Qtree**

Exibe o nome da qtree.

- **Cluster**

Exibe o nome do cluster que contém a qtree. Aparece apenas no ficheiro CSV exportado.

- **Storage Virtual Machine**

Exibe o nome da máquina virtual de storage (SVM) que contém a qtree. Aparece apenas no ficheiro CSV exportado.

- **Volume**

Exibe o nome do volume que contém a qtree.

Pode mover o ponteiro sobre o nome do volume para ver mais informações sobre o volume.

- **Conjunto de cotas**

Indica se uma cota está ativada ou desativada na qtree.

- **Tipo de cota**

Especifica se a cota é para um usuário, grupo de usuários ou uma qtree. Aparece apenas no ficheiro CSV exportado.

- **Usuário ou Grupo**

Exibe o nome do usuário ou grupo de usuários. Haverá várias linhas para cada usuário e grupo de usuários. Quando o tipo de cota é qtree ou se a cota não estiver definida, a coluna estará vazia. Aparece apenas no ficheiro CSV exportado.

- **Disco usado %**

Exibe a porcentagem de espaço em disco usado. Se um limite de disco rígido for definido, esse valor será baseado no limite de disco rígido. Se a cota for definida sem um limite de disco rígido, o valor será baseado no espaço de dados do volume. Se a cota não estiver definida ou se as cotas estiverem desativadas no volume ao qual a qtree pertence, então ""não aplicável"" é exibido na página da grade e o campo está em branco nos dados de exportação CSV.

- **Limite rígido do disco**

Exibe a quantidade máxima de espaço em disco alocado para a qtree. O Unified Manager gera um evento crítico quando esse limite é atingido e nenhuma gravação de disco adicional é permitida. O valor é exibido como "ilimitado" para as seguintes condições: Se a cota for definida sem um limite de disco rígido, se a cota não for definida ou se as cotas estiverem desativadas no volume a que a qtree pertence.

- **Limite de software do disco**

Exibe a quantidade de espaço em disco alocado para a qtree antes que um evento de aviso seja gerado. O valor é exibido como "ilimitado" para as seguintes condições: Se a cota for definida sem um limite de software do disco, se a cota não for definida ou se as cotas estiverem desativadas no volume a que a qtree pertence. Por padrão, essa coluna está oculta.

- **Limite do disco**

Exibe o valor de limite definido no espaço em disco. O valor é exibido como "ilimitado" para as seguintes condições: Se a cota for definida sem um limite de limite de disco, se a cota não for definida ou se as cotas estiverem desativadas no volume a que a qtree pertence. Por padrão, essa coluna está oculta.

- **Ficheiros utilizados %**

Exibe a porcentagem de arquivos usados na qtree. Se o limite rígido do arquivo estiver definido, esse valor será baseado no limite rígido do arquivo. Nenhum valor será exibido se a cota for definida sem um limite rígido de arquivo. Se a cota não estiver definida ou se as cotas estiverem desativadas no volume ao qual a qtree pertence, então ""não aplicável"" é exibido na página da grade e o campo está em branco nos dados de exportação CSV.

- **Limite rígido do arquivo**

Exibe o limite rígido para o número de arquivos permitidos no qtrees. O valor é exibido como "ilimitado" para as seguintes condições: Se a cota for definida sem um limite rígido de arquivo, se a cota não for definida, ou se as cotas estiverem desativadas no volume a que a qtree pertence.

- **Limite de software de arquivo**

Apresenta o limite de software para o número de ficheiros permitidos no qtrees. O valor é exibido como

"ilimitado" para as seguintes condições: Se a cota for definida sem um limite de arquivo, se a cota não for definida, ou se as cotas estiverem desativadas no volume a que a qtree pertence. Por padrão, essa coluna está oculta.

### Separador quotas de utilizador e grupo

Exibe detalhes sobre as cotas de usuário e grupo de usuários para a VM de armazenamento selecionada. Você pode exibir informações como o status da cota, nome do usuário ou grupo de usuários, limites físicos e físicos definidos nos discos e arquivos, quantidade de espaço em disco e número de arquivos usados e o valor de limite do disco. Você também pode alterar o endereço de e-mail associado a um usuário ou grupo de usuários.

- **Botão de comando Editar endereço de e-mail**

Abre a caixa de diálogo Editar endereço de e-mail, que exibe o endereço de e-mail atual do usuário ou grupo de usuários selecionado. Você pode modificar o endereço de e-mail. Se o campo **Editar endereço de e-mail** estiver em branco, a regra padrão será usada para gerar um endereço de e-mail para o usuário ou grupo de usuários selecionado.

Se mais de um usuário tiver a mesma cota, os nomes dos usuários serão exibidos como valores separados por vírgula. Além disso, a regra padrão não é usada para gerar o endereço de e-mail; portanto, você deve fornecer o endereço de e-mail necessário para que as notificações sejam enviadas.

- **Botão de comando Configurar regras de e-mail**

Permite criar ou modificar regras para gerar um endereço de e-mail para as cotas de usuário ou grupo de usuários configuradas na VM de armazenamento. Uma notificação é enviada para o endereço de e-mail especificado quando há uma violação de cota.

- **Status**

Exibe o status atual da cota. O estado pode ser crítico (❌), Aviso (⚠️) ou normal (✅).

Você pode mover o ponteiro sobre o ícone de status para exibir mais informações sobre o evento ou eventos gerados para a cota.

Se o status da cota for determinado por um único evento, você poderá exibir informações como o nome do evento, a hora e a data em que o evento foi acionado, o nome do administrador a quem o evento foi atribuído e a causa do evento. Você pode usar **Exibir detalhes** para ver mais informações sobre o evento.

Se o status da cota for determinado por vários eventos da mesma gravidade, os três principais eventos serão exibidos com informações como o nome do evento, a hora e a data em que os eventos foram acionados e o nome do administrador ao qual o evento foi atribuído. Você pode ver mais detalhes sobre cada um desses eventos clicando no nome do evento. Você também pode usar **Exibir todos os eventos** para visualizar a lista de eventos gerados.



Uma cota pode ter vários eventos da mesma gravidade ou severidades diferentes. No entanto, apenas a gravidade mais alta é exibida. Por exemplo, se uma cota tiver dois eventos com severidades de erro e aviso, somente a gravidade do erro será exibida.

- **Usuário ou Grupo**

Exibe o nome do usuário ou grupo de usuários. Se mais de um usuário tiver a mesma cota, os nomes dos usuários serão exibidos como valores separados por vírgula.

O valor é exibido como ""desconhecido"" quando o ONTAP não fornece um nome de usuário válido por causa de erros SecD.

- **Tipo**

Especifica se a cota é para um usuário ou um grupo de usuários.

- **Volume ou Qtree**

Exibe o nome do volume ou qtree em que a cota de usuário ou grupo de usuários é especificada.

Você pode mover o ponteiro sobre o nome do volume ou qtree para ver mais informações sobre o volume ou qtree.

- **Disco usado %**

Exibe a porcentagem de espaço em disco usado. O valor é exibido como ""não aplicável"" se a cota for definida sem um limite de disco rígido.

- **Limite rígido do disco**

Exibe a quantidade máxima de espaço em disco alocado para a cota. O Unified Manager gera um evento crítico quando esse limite é atingido e nenhuma gravação de disco adicional é permitida. O valor é exibido como "ilimitado" se a cota for definida sem um limite rígido do disco.

- **Limite de software do disco**

Exibe a quantidade de espaço em disco alocado para a cota antes que um evento de aviso seja gerado. O valor é exibido como "ilimitado" se a cota for definida sem um limite de software do disco. Por padrão, essa coluna está oculta.

- **Limite do disco**

Exibe o valor de limite definido no espaço em disco. O valor é exibido como "ilimitado" se a cota for definida sem um limite de limite de disco. Por padrão, essa coluna está oculta.

- **Ficheiros utilizados %**

Exibe a porcentagem de arquivos usados na qtree. O valor é exibido como ""não aplicável"" se a cota for definida sem um limite rígido de arquivo.

- **Limite rígido do arquivo**

Exibe o limite rígido para o número de arquivos permitidos na cota. O valor é exibido como "ilimitado" se a cota for definida sem um limite rígido de arquivo.

- **Limite de software de arquivo**

Exibe o limite de software para o número de arquivos permitidos na cota. O valor é exibido como "ilimitado" se a cota for definida sem um limite de software de arquivo. Por padrão, essa coluna está oculta.

- **Endereço de e-mail**

Exibe o endereço de e-mail do usuário ou grupo de usuários para o qual as notificações são enviadas quando há uma violação nas cotas.

## Guia compartilhamentos NFS

A guia compartilhamentos NFS exibe informações sobre compartilhamentos NFS, como seu status, o caminho associado ao volume (volumes FlexGroup ou volumes FlexVol), os níveis de acesso dos clientes aos compartilhamentos NFS e a política de exportação definida para os volumes exportados. Os compartilhamentos NFS não serão exibidos nas seguintes condições: Se o volume não estiver montado ou se os protocolos associados à política de exportação do volume não contiverem compartilhamentos NFS.

- **Status**

Exibe o status atual dos compartilhamentos NFS. O status pode ser erro (🚫) ou normal (✅).

- **Caminho de junção**

Apresenta o caminho para o qual o volume está montado. Se uma política explícita de exportações de NFS for aplicada a uma qtree, a coluna exibirá o caminho do volume pelo qual a qtree pode ser acessada.

- **Caminho de junção ativo**

Indica se o caminho para acessar ao volume montado está ativo ou inativo.

- **Volume ou Qtree**

Exibe o nome do volume ou qtree ao qual a política de exportação NFS é aplicada. Se uma política de exportação NFS for aplicada a uma qtree no volume, a coluna exibirá os nomes do volume e da qtree.

Você pode clicar no link para ver detalhes sobre o objeto na respectiva página de detalhes. Se o objeto for uma qtree, os links serão exibidos tanto para a qtree quanto para o volume.

- **Estado do volume**

Exibe o estado do volume que está sendo exportado. O estado pode ser Offline, Online, restrito ou Misto.

- Offline

O acesso de leitura ou gravação ao volume não é permitido.

- Online

O acesso de leitura e gravação ao volume é permitido.

- Restrito

Operações limitadas, como reconstrução de paridade, são permitidas, mas o acesso aos dados não é permitido.

- Misto

Os constituintes de um volume FlexGroup não estão todos no mesmo estado.

- **Estilo de segurança**

Exibe a permissão de acesso para os volumes exportados. O estilo de segurança pode ser UNIX, Unified, NTFS ou Misto.

- UNIX (clientes NFS)



Arquivos e diretórios no volume têm permissões UNIX.

- Unificado

Os arquivos e diretórios no volume têm um estilo de segurança unificado.

- NTFS (clientes CIFS)

Os arquivos e diretórios no volume têm permissões do Windows NTFS.

- Misto

Arquivos e diretórios no volume podem ter permissões UNIX ou permissões Windows NTFS.

- **Permissão UNIX**

Exibe os bits de permissão UNIX em um formato de cadeia de caracteres octal, que é definido para os volumes que são exportados. É semelhante aos bits de permissão do estilo UNIX.

- **Política de exportação**

Exibe as regras que definem a permissão de acesso para volumes exportados. Você pode clicar no link para exibir detalhes sobre as regras associadas à política de exportação, como os protocolos de autenticação e a permissão de acesso.

## Guia compartilhamentos SMB

Exibe informações sobre os compartilhamentos SMB na VM de storage selecionada. Você pode exibir informações como o status do compartilhamento SMB, nome do compartilhamento, caminho associado à VM de storage, o status do caminho de junção do compartilhamento, contendo objeto, estado do volume contendo, dados de segurança do compartilhamento e políticas de exportação definidas para o compartilhamento. Você também pode determinar se existe um caminho NFS equivalente para o compartilhamento SMB.



Compartilhamentos em pastas não são exibidos na guia compartilhamentos SMB.

- **Botão de comando View User Mapping**

Inicia a caixa de diálogo Mapeamento de usuários.

Você pode exibir os detalhes do mapeamento de usuários para a VM de armazenamento.

- **Mostrar botão de comando ACL**

Inicia a caixa de diálogo Controle de Acesso para o compartilhamento.

Você pode exibir os detalhes do usuário e da permissão para o compartilhamento selecionado.

- **Status**

Apresenta o estado atual da partilha. O status pode ser normal (✓) ou erro (!).

- **Nome da partilha**

Exibe o nome do compartilhamento SMB.

- **Caminho**

Apresenta o caminho de junção no qual a partilha é criada.

- **Caminho de junção ativo**

Exibe se o caminho para acessar o compartilhamento está ativo ou inativo.

- **Contendo Objeto**

Exibe o nome do objeto que contém ao qual o compartilhamento pertence. O objeto que contém pode ser um volume ou uma qtree.

Ao clicar no link, você pode visualizar detalhes sobre o objeto que contém na respectiva página Detalhes. Se o objeto que contém for uma qtree, os links serão exibidos para qtree e volume.

- **Estado do volume**

Exibe o estado do volume que está sendo exportado. O estado pode ser Offline, Online, restrito ou Misto.

- Offline

O acesso de leitura ou gravação ao volume não é permitido.

- Online

O acesso de leitura e gravação ao volume é permitido.

- Restrito

Operações limitadas, como reconstrução de paridade, são permitidas, mas o acesso aos dados não é permitido.

- Misto

Os constituintes de um volume FlexGroup não estão todos no mesmo estado.

- **Segurança**

Exibe a permissão de acesso para os volumes exportados. O estilo de segurança pode ser UNIX, Unified, NTFS ou Misto.

- UNIX (clientes NFS)

Arquivos e diretórios no volume têm permissões UNIX.

- Unificado

Os arquivos e diretórios no volume têm um estilo de segurança unificado.

- NTFS (clientes CIFS)

Os arquivos e diretórios no volume têm permissões do Windows NTFS.

- Misto

Arquivos e diretórios no volume podem ter permissões UNIX ou permissões Windows NTFS.

- **Política de exportação**

Exibe o nome da política de exportação aplicável ao compartilhamento. Se uma política de exportação não for especificada para a VM de armazenamento, o valor será exibido como não ativado.

Você pode clicar no link para exibir detalhes sobre as regras associadas à política de exportação, como protocolos de acesso e permissões. O link será desativado se a política de exportação estiver desativada para a VM de armazenamento selecionada.

- **Equivalente NFS**

Especifica se existe um equivalente NFS para o compartilhamento.

## Guia San

Exibe detalhes sobre LUNs, grupos de iniciadores e iniciadores para a VM de armazenamento selecionada. Por predefinição, é apresentada a vista LUNs. Você pode exibir detalhes sobre os grupos de iniciadores na guia grupos de iniciadores e detalhes sobre iniciadores na guia iniciadores.

- **Separador LUNs**

Exibe detalhes sobre os LUNs que pertencem à VM de armazenamento selecionada. Pode visualizar informações como o nome do LUN, o estado do LUN (online ou offline), o nome do sistema de arquivos (volume ou qtree) que contém o LUN, o tipo de sistema operativo anfitrião, a capacidade total de dados e o número de série do LUN. A coluna desempenho de LUN fornece um link para a página de detalhes de LUN/desempenho.

Você também pode exibir informações se o provisionamento de thin está habilitado no LUN e se o LUN é mapeado para um grupo de iniciadores. Se for mapeado para um iniciador, você poderá exibir os grupos de iniciadores e iniciadores que são mapeados para o LUN selecionado.

- **Separador grupos de iniciadores**

Exibe detalhes sobre os grupos de iniciadores. Você pode exibir detalhes como o nome do grupo de iniciadores, o estado de acesso, o tipo de sistema operacional do host que é usado por todos os iniciadores do grupo e o protocolo suportado. Quando você clica no link na coluna Estado de acesso, você pode exibir o estado de acesso atual do grupo de iniciadores.

- **Normal**

- O grupo de iniciadores está conectado a vários caminhos de acesso.

- **Caminho único**

- O grupo de iniciadores está conectado a um único caminho de acesso.

- **Sem caminhos**

- Não existe um caminho de acesso ligado ao grupo de iniciadores.

Você pode ver se os grupos de iniciadores são mapeados para todas as interfaces ou interfaces específicas por meio de um conjunto de portas. Quando você clica no link contagem na coluna interfaces mapeadas, todas as interfaces são exibidas ou interfaces específicas para um conjunto de

portas são exibidas. As interfaces que são mapeadas através do portal de destino não são exibidas. É apresentado o número total de iniciadores e LUNs mapeados para um grupo de iniciadores.

Você também pode exibir os LUNs e iniciadores que são mapeados para o grupo de iniciadores selecionado.

- **Separador iniciadores**

Exibe o nome e o tipo do iniciador e o número total de grupos de iniciadores mapeados para este iniciador para a VM de armazenamento selecionada.

```
initiator groups that are mapped to the selected initiator group.
```

#### **Painel Anotações relacionadas**

O painel Anotações relacionadas permite visualizar os detalhes da anotação associados à VM de armazenamento selecionada. Os detalhes incluem o nome da anotação e os valores da anotação que são aplicados à VM de armazenamento. Também pode remover anotações manuais do painel Anotações relacionadas.

#### **Painel dispositivos relacionados**

O painel dispositivos relacionados permite visualizar o cluster, agregados e volumes relacionados à VM de storage:

- **Cluster**

Exibe o status de integridade do cluster ao qual a VM de armazenamento pertence.

- **Agregados**

Exibe o número de agregados que pertencem à VM de storage selecionada. O estado de saúde dos agregados também é exibido, com base no nível de gravidade mais alto. Por exemplo, se uma VM de armazenamento contiver dez agregados, cinco dos quais exibem o status de aviso e os cinco restantes exibem o status crítico, então o status exibido é crítico.

- **Agregados atribuídos**

Exibe o número de agregados atribuídos a uma VM de storage. O estado de saúde dos agregados também é exibido, com base no nível de gravidade mais alto.

- **Volumes**

Exibe o número e a capacidade dos volumes que pertencem à VM de armazenamento selecionada. O estado de funcionamento dos volumes também é apresentado, com base no nível de gravidade mais elevado. Quando há volumes FlexGroup na VM de armazenamento, a contagem também inclui FlexGroups; ela não inclui componentes FlexGroup.

#### **Painel grupos relacionados**

O painel grupos relacionados permite exibir a lista de grupos associados à VM de armazenamento selecionada.

## Painel Alertas relacionados

O painel Alertas relacionados permite exibir a lista de alertas criados para a VM de storage selecionada. Você também pode adicionar um alerta clicando no link **Adicionar alerta** ou editar um alerta existente clicando no nome do alerta.

## Página de detalhes de cluster / Saúde

A página de detalhes de cluster/integridade fornece informações detalhadas sobre um cluster selecionado, como detalhes de integridade, capacidade e configuração. Você também pode exibir informações sobre as interfaces de rede (LIFs), nós, discos, dispositivos relacionados e alertas relacionados para o cluster.

O status ao lado do nome do cluster, por exemplo (bom), representa o status da comunicação; se o Unified Manager pode se comunicar com o cluster. Ele não representa o status de failover ou o status geral do cluster.

## Botões de comando

Os botões de comando permitem executar as seguintes tarefas para o cluster selecionado:

- **Mude para a visualização de desempenho**

Permite-lhe navegar para a página de detalhes de Cluster / Performance.

- **Ações**

- Adicionar alerta: Abre a caixa de diálogo Adicionar alerta, que permite adicionar um alerta ao cluster selecionado.
- Redescobrir: Inicia uma atualização manual do cluster, que permite ao Unified Manager descobrir alterações recentes no cluster.

Se o Unified Manager estiver emparelhado com o OnCommand Workflow Automation, a operação de redescoberta também readquire dados em cache DO WFA, se houver.

Após a operação de redescoberta ser iniciada, é apresentado um link para os detalhes do trabalho associado para permitir o controle do estado do trabalho.

- Anotar: Permite anotar o cluster selecionado.

- **View clusters**

Permite navegar para a visualização Saúde: Todos os clusters.

## Separador Saúde

Exibe informações detalhadas sobre problemas de disponibilidade de dados e capacidade de dados de vários objetos de cluster, como nós, SVMs e agregados. Os problemas de disponibilidade estão relacionados à funcionalidade de fornecimento de dados dos objetos do cluster. Os problemas de capacidade estão relacionados à capacidade de armazenamento de dados dos objetos do cluster.

Você pode clicar no gráfico de um objeto para exibir uma lista filtrada dos objetos. Por exemplo, você pode clicar no gráfico de capacidade SVM que exibe avisos para exibir uma lista filtrada de SVMs. Esta lista contém SVMs que têm volumes ou qtrees que têm problemas de capacidade com um nível de gravidade de Aviso. Você também pode clicar no gráfico de disponibilidade SVMs que exibe avisos para exibir a lista de SVMs que

têm problemas de disponibilidade com um nível de gravidade de Aviso.

## Problemas de disponibilidade

Exibe graficamente o número total de objetos, incluindo objetos que têm problemas de disponibilidade e objetos que não têm problemas relacionados à disponibilidade. As cores no gráfico representam os diferentes níveis de gravidade dos problemas. As informações abaixo do gráfico fornecem detalhes sobre problemas de disponibilidade que podem afetar ou que já afetaram a disponibilidade de dados no cluster. Por exemplo, são exibidas informações sobre compartimentos de disco inativos e agregados offline.



Os dados exibidos para o gráfico de barras SFO são baseados no estado de HA dos nós. Os dados apresentados para todos os outros gráficos de barras são calculados com base nos eventos gerados.

## Problemas de capacidade

Exibe graficamente o número total de objetos, incluindo objetos que têm problemas de capacidade e objetos que não têm problemas relacionados à capacidade. As cores no gráfico representam os diferentes níveis de gravidade dos problemas. As informações abaixo do gráfico fornecem detalhes sobre problemas de capacidade que podem afetar ou que já afetaram a capacidade dos dados no cluster. Por exemplo, informações são exibidas sobre agregados que provavelmente violarão os valores de limite definidos.

### Separador capacidade

Exibe informações detalhadas sobre a capacidade do cluster selecionado.

## Capacidade

Exibe o gráfico de capacidade de dados sobre a capacidade usada e a capacidade disponível de todos os agregados alocados:

- Espaço lógico utilizado

O tamanho real dos dados que estão sendo armazenados em todos os agregados neste cluster sem aplicar as economias com o uso das tecnologias de eficiência de storage da ONTAP. Isso não inclui cópias Snapshot.

- Redução de dados

Exibe a proporção sem cópias Snapshot e com dois dígitos significativos, por exemplo, 1,8 a 1. Essa taxa é baseada nas configurações de eficiência de storage do ONTAP configuradas.

- Usado

A capacidade física utilizada pelos dados em todos os agregados. Isso não inclui a capacidade usada para paridade, dimensionamento correto e reserva.

- Disponível

Exibe a capacidade disponível para os dados.

- Peças sobressalentes

Exibe a capacidade armazenável disponível para armazenamento em todos os discos sobressalentes.

- Provisionado

Exibe a capacidade provisionada para todos os volumes subjacentes.

## Detalhes

Apresenta informações detalhadas sobre a capacidade utilizada e disponível. O cálculo exclui os dados agregados de raiz.

- Capacidade total

Exibe a capacidade total do cluster. Isso não inclui a capacidade atribuída para paridade.

- Usado

Exibe a capacidade usada pelos dados. Isso não inclui a capacidade usada para paridade, dimensionamento correto e reserva.

- Disponível

Exibe a capacidade disponível para os dados.

- Provisionado

Exibe a capacidade provisionada para todos os volumes subjacentes.

- Peças sobressalentes

Exibe a capacidade armazenável disponível para armazenamento em todos os discos sobressalentes.

## Camada de nuvem

Exibe a capacidade total da camada de nuvem usada e a capacidade usada para cada camada de nuvem conetada para agregados habilitados para FabricPool no cluster. Um FabricPool pode ser licenciado ou não licenciado.

## Capacidade física Breakout por tipo de disco

A área Physical Capacity Breakout by Disk Type (quebra de capacidade física por tipo de disco) exibe informações detalhadas sobre a capacidade de disco dos vários tipos de discos no cluster. Ao clicar no tipo de disco, você pode exibir mais informações sobre o tipo de disco na guia discos.

- Capacidade utilizável total

Exibe a capacidade disponível e a capacidade sobressalente dos discos de dados.

- HDD

Apresenta graficamente a capacidade utilizada e a capacidade disponível de todos os discos de dados HDD no cluster. A linha pontilhada representa a capacidade sobressalente dos discos de dados no HDD.

- Flash

- Dados SSD

Exibe graficamente a capacidade usada e a capacidade disponível dos discos de dados SSD no cluster.

- Cache SSD

Exibe graficamente a capacidade armazenável dos discos de cache SSD no cluster.

- SSD sobresselente

Exibe graficamente a capacidade sobressalente dos discos SSD, dados e cache no cluster.

- Discos não atribuídos

Exibe o número de discos não atribuídos no cluster.

## Lista de agregados com problemas de capacidade

Exibe detalhes em formato tabular sobre a capacidade usada e a capacidade disponível dos agregados que têm problemas de risco de capacidade.

- Estado

Indica que o agregado tem um problema relacionado à capacidade de uma determinada gravidade.

Você pode mover o ponteiro sobre o status para exibir mais informações sobre o evento ou eventos gerados para o agregado.

Se o status do agregado for determinado por um único evento, você poderá exibir informações como o nome do evento, a hora e a data em que o evento foi acionado, o nome do administrador a quem o evento foi atribuído e a causa do evento. Você pode clicar no botão **Exibir detalhes** para ver mais informações sobre o evento.

Se o status do agregado for determinado por vários eventos da mesma gravidade, os três principais eventos serão exibidos com informações como o nome do evento, a hora e a data em que os eventos são acionados e o nome do administrador a quem o evento é atribuído. Você pode ver mais detalhes sobre cada um desses eventos clicando no nome do evento. Você também pode clicar no link **Exibir todos os eventos** para visualizar a lista de eventos gerados.



Um agregado pode ter vários eventos relacionados à capacidade da mesma gravidade ou gravidades diferentes. No entanto, apenas a gravidade mais alta é exibida. Por exemplo, se um agregado tiver dois eventos com níveis de gravidade de erro e crítico, somente a gravidade Crítica será exibida.

- Agregado

Exibe o nome do agregado.

- Capacidade de dados utilizada

Exibe graficamente informações sobre o uso de capacidade agregada (em porcentagem).

- Dias para cheio

Exibe o número estimado de dias restantes antes que o agregado atinja a capacidade total.



## Separador Configuration (Configuração)

Exibe detalhes sobre o cluster selecionado, como endereço IP, Contato e localização:

### Visão geral do cluster

- Interface de gerenciamento

Exibe o LIF de gerenciamento de cluster que o Unified Manager usa para se conectar ao cluster. O estado operacional da interface também é exibido.

- Nome do host ou endereço IP

Exibe o FQDN, o nome abreviado ou o endereço IP do LIF de gerenciamento de cluster que o Unified Manager usa para se conectar ao cluster.

- FQDN

Exibe o nome de domínio totalmente qualificado (FQDN) do cluster.

- Versão do SO

Exibe a versão do ONTAP que o cluster está sendo executado. Se os nós do cluster estiverem executando versões diferentes do ONTAP, a versão mais antiga do ONTAP será exibida.

- Contacto

Apresenta detalhes sobre o administrador a quem deve contactar em caso de problemas com o cluster.

- Localização

Apresenta a localização do cluster.

- Personalidade

Identifica se este é um cluster configurado para All SAN Array.

### Visão geral do cluster remoto

Fornecer detalhes sobre o cluster remoto em uma configuração do MetroCluster. Esta informação é apresentada apenas para as configurações do MetroCluster.

- Cluster

Exibe o nome do cluster remoto. Pode clicar no nome do cluster para navegar para a página de detalhes do cluster.

- Nome do host ou endereço IP

Exibe o FQDN, o nome curto ou o endereço IP do cluster remoto.

- Localização

Apresenta a localização do cluster remoto.

## Visão geral do MetroCluster

Fornecer detalhes sobre o cluster local em configurações de MetroCluster em FC ou MetroCluster em IP. Essas informações são exibidas apenas para configurações MetroCluster em FC ou IP.

- Tipo

Exibe se o tipo MetroCluster é de dois nós ou quatro nós. Para MetroCluster sobre IP, apenas quatro nós são suportados.

- Configuração

Exibe a configuração do MetroCluster em FC e IP, que podem ter os seguintes valores:

### Para FC

- Configuração elástica com cabos SAS
- Configuração elástica com ponte FC-SAS
- Configuração de malha com switches FC



Para um MetroCluster de quatro nós, somente a configuração de malha com switches FC é compatível.

### Para IP

- Configuração IP com switches Ethernet (L2 ou L3, dependendo de como o cluster é configurado)
  - Comutador não planejado automatizado (AUSO)

Exibe se o switchover automatizado não planejado está ativado para o cluster local. Por padrão, o AUSO é habilitado para todos os clusters em uma configuração de MetroCluster de dois nós no Unified Manager. Você pode usar a interface de linha de comando para alterar a configuração AUSO. Isso é compatível apenas com MetroCluster em FC.

- Modo de comutação

Apresenta o modo de comutação para a configuração MetroCluster over IP. Os valores disponíveis são: `Active`, `Negotiated Switchover`, e `Automatic Unplanned Switchover`.

### Nós

- Disponibilidade

Exibe o número de nós que estão para cima (●) ou para baixo (●) no cluster.

- Versões do SO

Exibe as versões do ONTAP que os nós estão sendo executados, bem como o número de nós que executam uma versão específica do ONTAP. Por exemplo, 9,6 (2), 9,3 (1) especifica que dois nós estão executando o ONTAP 9.6 e um nó está executando o ONTAP 9.3.

## Máquinas virtuais de armazenamento

- Disponibilidade

Exibe o número de SVMs que estão para cima (●) ou para baixo (●) no cluster.

## Interfaces de rede

- Disponibilidade

Exibe o número de LIFs não-dados que estão para cima (●) ou para baixo (●) no cluster.

- Interfaces de gerenciamento de clusters

Exibe o número de LIFs de gerenciamento de cluster.

- Interfaces de gerenciamento de nós

Exibe o número de LIFs de gerenciamento de nós.

- Interfaces de cluster

Exibe o número de LIFs de cluster.

- Interfaces entre clusters

Exibe o número de LIFs entre clusters.

## Protocolos

- Protocolos de dados

Exibe a lista de protocolos de dados licenciados que estão habilitados para o cluster. Os protocolos de dados incluem iSCSI, CIFS, NFS, NVMe e FC/FCoE.

## Proteção

- Mediadores

Exibe se o cluster suporta mediadores e o status de conectividade do mediador. Indica se o mediador está configurado e, se configurado, exibe o status dos mediadores.

- Não aplicável

É apresentado quando o cluster não suporta mediadores.

- Não configurado

É exibido quando o cluster suporta mediadores, mas o mediador não está configurado.

- Endereço IP

É exibido quando o cluster suporta mediadores e o mediador está configurado. O status do mediador é indicado por cor. A cor verde indica que o status do mediador está acessível. A cor vermelha indica

que o status do mediador não está acessível.

## Categorias de nuvem

Lista os nomes dos níveis de nuvem aos quais esse cluster está conectado. Ele também lista o tipo (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage ou StorageGRID) e os estados das camadas de nuvem (disponíveis ou indisponíveis).

## Separador conectividade MetroCluster

Exibe os problemas e o status de conectividade dos componentes do cluster na configuração MetroCluster sobre FC. Um cluster é exibido em uma caixa vermelha quando o parceiro de recuperação de desastres do cluster tiver problemas.



A guia conectividade do MetroCluster é exibida somente para clusters que estão em uma configuração MetroCluster sobre FC.

Pode navegar para a página de detalhes de um cluster remoto clicando no nome do cluster remoto. Você também pode visualizar os detalhes dos componentes clicando no link contagem de um componente. Por exemplo, clicar no link contagem do nó no cluster exibe a guia nó na página de detalhes do cluster. Clicar no link contagem dos discos no cluster remoto exibe a guia disco na página de detalhes do cluster remoto.



Ao gerenciar uma configuração de MetroCluster de oito nós, clicar no link contagem do componente shelves de disco exibe apenas as gavetas locais do par de HA padrão. Além disso, não há como exibir as gavetas locais no outro par de HA.

Você pode mover o ponteiro sobre os componentes para exibir os detalhes e o status de conectividade dos clusters em caso de qualquer problema e para exibir mais informações sobre o evento ou eventos gerados para o problema.

Se o status do problema de conectividade entre componentes for determinado por um único evento, você poderá exibir informações como o nome do evento, a hora e a data em que o evento foi acionado, o nome do administrador a quem o evento foi atribuído e a causa do evento. O botão Ver Detalhes fornece mais informações sobre o evento.

Se o status do problema de conectividade entre componentes for determinado por vários eventos da mesma gravidade, os três principais eventos serão exibidos com informações como o nome do evento, a hora e a data em que os eventos são acionados e o nome do administrador a quem o evento é atribuído. Você pode ver mais detalhes sobre cada um desses eventos clicando no nome do evento. Você também pode clicar no link **Exibir todos os eventos** para visualizar a lista de eventos gerados.

## Guia replicação do MetroCluster

Exibe o status dos dados que estão sendo replicados em uma configuração MetroCluster em FC. Você pode usar a guia replicação do MetroCluster para garantir a proteção de dados espelhando os dados de maneira síncrona com os clusters já direcionados. Um cluster é exibido em uma caixa vermelha quando o parceiro de recuperação de desastres do cluster tiver problemas.



A guia replicação do MetroCluster é exibida somente para clusters que estão em uma configuração MetroCluster sobre FC.

Em um ambiente MetroCluster, você pode usar essa guia para verificar as conexões lógicas e o peering do cluster local com o cluster remoto. Você pode exibir a representação objetiva dos componentes do cluster com

suas conexões lógicas. Isso ajuda a identificar os problemas que podem ocorrer durante o espelhamento de metadados e dados.

Na guia replicação do MetroCluster , o cluster local fornece a representação gráfica detalhada do cluster selecionado e o parceiro do MetroCluster refere-se ao cluster remoto.




### **Separador interfaces de rede**

Exibe detalhes sobre todas as LIFs que não são de dados criados no cluster selecionado.




### **Interface de rede**

Exibe o nome do LIF criado no cluster selecionado.

### **Estado operacional**

Exibe o status operacional da interface, que pode ser para cima (  ), para baixo (  ) ou desconhecido (  ). O status operacional de uma interface de rede é determinado pelo status de suas portas físicas.

### **Estado administrativo**

Exibe o status administrativo da interface, que pode ser para cima (  ), para baixo (  ) ou desconhecido (  ). Você pode controlar o status administrativo de uma interface ao fazer alterações na configuração ou durante a manutenção. O estado administrativo pode ser diferente do estado operacional. No entanto, se o status administrativo de um LIF estiver inativo, o status operacional estará inativo por padrão.

### **Endereço IP**

Apresenta o endereço IP da interface.

### **Função**

Exibe a função da interface. As funções possíveis são LIFs de gerenciamento de clusters, LIFs de gerenciamento de nós, LIFs de cluster e LIFs de Intercluster.

### **Porta inicial**

Exibe a porta física à qual a interface foi originalmente associada.

### **Porta atual**

Exibe a porta física à qual a interface está atualmente associada. Após a migração de LIF, a porta atual pode ser diferente da porta inicial.

### **Política de failover**

Exibe a política de failover configurada para a interface.

### **Grupos de roteamento**

Exibe o nome do grupo de roteamento. Você pode exibir mais informações sobre as rotas e o gateway de destino clicando no nome do grupo de roteamento.

Os grupos de roteamento não são compatíveis com o ONTAP 8,3 ou posterior e, portanto, uma coluna em branco é exibida para esses clusters.

## Grupo de failover

Exibe o nome do grupo de failover.

### Guia nós

Exibe informações sobre nós no cluster selecionado. Você pode visualizar informações detalhadas sobre pares de HA, compartimentos de disco e portas:

### Detalhes HA

Fornece uma representação pictórica do estado de HA e do estado de saúde dos nós no par de HA. O estado de funcionamento do nó é indicado pelas seguintes cores:

- **Verde**

O nó está em uma condição de trabalho.

- **Amarelo**

O nó assumiu o nó do parceiro ou o nó está enfrentando alguns problemas ambientais.

- **Vermelho**

O nó está inativo.

Você pode visualizar informações sobre a disponibilidade do par de HA e tomar as medidas necessárias para evitar riscos. Por exemplo, no caso de uma possível operação de aquisição, a seguinte mensagem é exibida: Failover de armazenamento possível.

Você pode exibir uma lista dos eventos relacionados ao par de HA e ao seu ambiente, como ventiladores, fontes de alimentação, bateria NVRAM, placas flash, processador de serviço e conectividade de compartimentos de disco. Você também pode ver a hora em que os eventos foram acionados.

Você pode visualizar outras informações relacionadas ao nó, como o número do modelo.

Se houver clusters de nó único, você também poderá exibir detalhes sobre os nós.

## Compartimentos de disco

Exibe informações sobre os compartimentos de disco no par de HA.

Você também pode exibir eventos gerados para as gavetas de disco e os componentes ambientais, bem como a hora em que os eventos foram acionados.

- **ID da prateleira**

Exibe a ID da prateleira onde o disco está localizado.

- **Status do componente**

Exibe detalhes ambientais das prateleiras de disco, como fontes de alimentação, ventiladores, sensores de temperatura, sensores de corrente, conectividade de disco e sensores de tensão. Os detalhes ambientais são apresentados como ícones nas seguintes cores:

- **Verde**

Os componentes ambientais estão funcionando corretamente.

- **Cinza**

Não há dados disponíveis para os componentes ambientais.

- **Vermelho**

Alguns dos componentes ambientais estão em baixo.

- **Estado**

Exibe o estado do compartimento de disco. Os estados possíveis são Offline, Online, no status, Initialization required, Missing, and Unknown.

- **Modelo**

Exibe o número do modelo do compartimento de disco.

- **Compartimento de disco local**

Indica se o compartimento de disco está localizado no cluster local ou no cluster remoto. Essa coluna é exibida somente para clusters em uma configuração do MetroCluster.

- \* ID exclusivo\*

Exibe o identificador exclusivo do compartimento de disco.

- **Versão do firmware**

Exibe a versão do firmware do compartimento de disco.

## Portas

Exibe informações sobre as portas FC, FCoE e Ethernet associadas. Você pode exibir detalhes sobre as portas e os LIFs associados clicando nos ícones de porta.

Você também pode exibir os eventos gerados para as portas.

Você pode exibir os seguintes detalhes da porta:

- ID da porta

Exibe o nome da porta. Por exemplo, os nomes das portas podem ser e0M, e0a e e0b.

- Função

Exibe a função da porta. As funções possíveis são Cluster, Data, Intercluster, Node-Management e Undefined.

- Tipo

Exibe o protocolo da camada física usado para a porta. Os tipos possíveis são Ethernet, Fibre Channel e FCoE.

- WWPN

Exibe o nome da porta mundial (WWPN) da porta.

- Rev. Do firmware

Exibe a revisão de firmware da porta FC/FCoE.

- Estado

Exibe o estado atual da porta. Os estados possíveis são para cima, para baixo, ligação não ligada ou desconhecido (?).

Pode visualizar os eventos relacionados com portas a partir da lista Eventos. Você também pode exibir os detalhes de LIF associados, como nome de LIF, status operacional, endereço IP ou WWPN, protocolos, nome do SVM associado ao LIF, porta atual, política de failover e grupo de failover.

### **Separador Disks (discos)**

Exibe detalhes sobre os discos no cluster selecionado. Você pode exibir informações relacionadas ao disco, como o número de discos usados, discos sobressalentes, discos quebrados e discos não atribuídos. Você também pode exibir outros detalhes, como o nome do disco, o tipo de disco e o nó proprietário do disco.

### **Resumo do pool de discos**

Exibe o número de discos, que são categorizados por tipos efetivos (FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN e VMDISK) e o estado dos discos. Você também pode exibir outros detalhes, como o número de agregados, discos compartilhados, discos sobressalentes, discos quebrados, discos não atribuídos e discos não suportados. Se você clicar no link contagem efetiva do tipo de disco, os discos do estado selecionado e do tipo efetivo serão exibidos. Por exemplo, se você clicar no link contagem do estado do disco quebrado e do tipo SAS efetivo, todos os discos com o estado do disco quebrado e SAS do tipo efetivo serão exibidos.

### **Disco**

Exibe o nome do disco.

### **Grupos RAID**

Exibe o nome do grupo RAID.

### **Nó proprietário**

Exibe o nome do nó ao qual o disco pertence. Se o disco não estiver atribuído, nenhum valor será exibido nesta coluna.

### **Estado**

Exibe o estado do disco: Agregado, compartilhado, sobressalente, quebrado, não atribuído, não suportado ou desconhecido. Por padrão, essa coluna é classificada para exibir os estados na seguinte ordem: Quebrado, não atribuído, não suportado, sobressalente, agregado e compartilhado.



## **Disco local**

Exibe Sim ou não para indicar se o disco está localizado no cluster local ou no cluster remoto. Essa coluna é exibida somente para clusters em uma configuração do MetroCluster.

## **Posição**

Exibe a posição do disco com base em seu tipo de contentor: Por exemplo, cópia, dados ou paridade. Por padrão, essa coluna está oculta.

## **Agregados impactados**

Exibe o número de agregados que são afetados devido ao disco com falha. Você pode mover o ponteiro sobre o link de contagem para exibir os agregados afetados e, em seguida, clicar no nome do agregado para exibir detalhes do agregado. Você também pode clicar na contagem de agregados para visualizar a lista de agregados impactados na visualização Saúde: Todos agregados.

Nenhum valor é exibido nesta coluna para os seguintes casos:

- Para discos quebrados quando um cluster contendo esses discos é adicionado ao Unified Manager
- Quando não há discos com falha

## **Pool de storage**

Exibe o nome do pool de armazenamento ao qual o SSD pertence. Você pode mover o ponteiro sobre o nome do pool de armazenamento para exibir detalhes do pool de armazenamento.

## **Capacidade armazenável**

Exibe a capacidade do disco disponível para uso.

## **Capacidade bruta**

Exibe a capacidade do disco bruto e não formatado antes do dimensionamento correto e da configuração RAID. Por padrão, essa coluna está oculta.

## **Tipo**

Exibe os tipos de discos: Por exemplo, ATA, SATA, FCAL ou VMDISK.

## **Tipo eficaz**

Exibe o tipo de disco atribuído pelo ONTAP.

Certos tipos de disco ONTAP são considerados equivalentes para criar e adicionar agregados e gerenciamento de reserva. O ONTAP atribui um tipo de disco efetivo para cada tipo de disco.

## **Blocos de reposição consumidos %**

Exibe em porcentagem os blocos sobressalentes que são consumidos no disco SSD. Esta coluna está em branco para discos que não sejam discos SSD.

## **Vida nominal utilizada %**

Exibe em porcentagem uma estimativa da vida útil do SSD usada, com base no uso real do SSD e na previsão do fabricante da vida útil do SSD. Um valor superior a 99 indica que a resistência estimada foi consumida, mas pode não indicar falha no SSD. Se o valor for desconhecido, o disco será omitido.

## **Firmware**

Apresenta a versão do firmware do disco.

## **RPM**

Apresenta as rotações por minuto (RPM) do disco. Por padrão, essa coluna está oculta.

## **Modelo**

Exibe o número do modelo do disco. Por padrão, essa coluna está oculta.

## **Fornecedor**

Exibe o nome do fornecedor do disco. Por padrão, essa coluna está oculta.

## **ID do compartimento**

Exibe a ID da prateleira onde o disco está localizado.

## **Baía**

Exibe a ID do compartimento onde o disco está localizado.

## **Painel Anotações relacionadas**

Permite visualizar os detalhes da anotação associados ao cluster selecionado. Os detalhes incluem o nome da anotação e os valores da anotação que são aplicados ao cluster. Também pode remover anotações manuais do painel Anotações relacionadas.

## **Painel dispositivos relacionados**

Permite visualizar detalhes do dispositivo associados ao cluster selecionado.

Os detalhes incluem propriedades do dispositivo conectado ao cluster, como tipo, tamanho, contagem e status de integridade do dispositivo. Você pode clicar no link contagem para mais análises sobre esse dispositivo específico.

Use o painel de parceiros do MetroCluster para obter contagem e detalhes sobre o parceiro MetroCluster remoto, além de seus componentes de cluster associados, como nós, agregados e SVMs. O painel de parceiros do MetroCluster é exibido apenas para clusters em uma configuração do MetroCluster.

O painel dispositivos relacionados permite visualizar e navegar para os nós, SVMs e agregados relacionados ao cluster:

## **Parceiro MetroCluster**

Exibe o status de integridade do parceiro MetroCluster. Usando o link contagem, você pode navegar mais longe e obter informações sobre a integridade e a capacidade dos componentes do cluster.

## Nós

Exibe o número, a capacidade e o status de integridade dos nós que pertencem ao cluster selecionado. Capacidade indica a capacidade utilizável total em relação à capacidade disponível.

## Máquinas virtuais de armazenamento

Exibe o número de SVMs que pertencem ao cluster selecionado.

## Agregados

Exibe o número, a capacidade e o status de integridade dos agregados que pertencem ao cluster selecionado.

## Painel grupos relacionados

Permite visualizar a lista de grupos que inclui o cluster selecionado.

## Painel Alertas relacionados

O painel Alertas relacionados permite visualizar a lista de alertas para o cluster selecionado. Você também pode adicionar um alerta clicando no link Adicionar alerta ou editar um alerta existente clicando no nome do alerta.

## Informações relacionadas

["Página volumes"](#) ["Visualizar a lista de cluster e os detalhes"](#)

## Página de detalhes agregados / Saúde

Você pode usar a página de detalhes de agregado / integridade para exibir informações detalhadas sobre o agregado selecionado, como a capacidade, informações de disco, detalhes de configuração e eventos gerados. Você também pode exibir informações sobre os objetos relacionados e alertas relacionados para esse agregado.

## Botões de comando



Ao monitorar um agregado habilitado para FabricPool, os valores comprometidos e supercomprometidos nesta página são relevantes somente para a capacidade local ou do nível de desempenho. A quantidade de espaço disponível na camada de nuvem não se reflete em valores supercomprometidos. Da mesma forma, os valores de limite agregados são relevantes apenas para o nível de desempenho local.

Os botões de comando permitem executar as seguintes tarefas para o agregado selecionado:

- **Mude para a visualização de desempenho**

Permite-lhe navegar para a página de detalhes de agregação/desempenho.

- **Ações**

- Adicionar alerta

Permite adicionar um alerta ao agregado selecionado.

- Editar limites

Permite modificar as definições de limite para o agregado selecionado.

- **Ver agregados**

Permite navegar para a visualização Saúde: Todos os agregados.

### **Separador capacidade**

A guia capacidade exibe informações detalhadas sobre o agregado selecionado, como sua capacidade, limites e taxa de crescimento diária.

Por padrão, eventos de capacidade não são gerados para agregados raiz. Além disso, os valores de limite usados pelo Unified Manager não são aplicáveis a agregados de raiz de nós. Somente um representante de suporte técnico pode modificar as configurações para que esses eventos sejam gerados. Quando as configurações são modificadas por um representante de suporte técnico, os valores de limite são aplicados ao agregado raiz do nó.

- **Capacidade**

Exibe o gráfico de capacidade de dados e o gráfico cópias Snapshot, que exibe detalhes de capacidade sobre o agregado:

- Espaço lógico utilizado

O tamanho real dos dados que estão sendo armazenados no agregado sem aplicar a economia com o uso das tecnologias de eficiência de storage da ONTAP.

- Usado

A capacidade física utilizada pelos dados no agregado.

- Compromisso excessivo

Quando o espaço no agregado é supercomprometido, o gráfico exibe um sinalizador com o valor supercomprometido.

- Aviso

Exibe uma linha pontilhada no local onde o limite de aviso está definido; o que significa que o espaço no agregado está quase cheio. Se esse limite for violado, o evento espaço quase cheio será gerado.

- Erro

Exibe uma linha sólida no local onde o limite de erro é definido; o que significa que o espaço no agregado está cheio. Se esse limite for violado, o evento espaço cheio será gerado.

- Gráfico de cópias Snapshot

Este gráfico é exibido apenas quando a capacidade Snapshot usada ou a reserva Instantânea não é zero.

Ambos os gráficos exibem a capacidade pela qual a capacidade de captura instantânea excede a reserva de captura instantânea se a capacidade de captura instantânea usada exceder a reserva de captura

instantânea.

- **Nível de nuvem**

Exibe o espaço usado pelos dados na camada de nuvem para agregados habilitados para FabricPool. Um FabricPool pode ser licenciado ou não licenciado.

Quando o nível de nuvem é espelhado para outro provedor de nuvem (o "nível de erro"), ambos os níveis de nuvem são exibidos aqui.

- **Detalhes**

Exibe informações detalhadas sobre a capacidade.

- Capacidade total

Exibe a capacidade total no agregado.

- Capacidade de dados

Exibe a quantidade de espaço usada pelo agregado (capacidade usada) e a quantidade de espaço disponível no agregado (capacidade livre).

- Reserva do Snapshot

Exibe a capacidade Snapshot usada e livre do agregado.

- Capacidade excedentária

Exibe o comprometimento agregado em excesso. O comprometimento em excesso agregado permite que você forneça mais storage do que realmente disponível em um determinado agregado, contanto que nem todo esse storage esteja sendo usado no momento. Quando o thin Provisioning está em uso, o tamanho total dos volumes no agregado pode exceder a capacidade total do agregado.



Se você tiver sobrecarregado seu agregado, você deve monitorar o espaço disponível cuidadosamente e adicionar armazenamento conforme necessário para evitar erros de gravação devido a espaço insuficiente.

- Camada de nuvem

Exibe o espaço usado pelos dados na camada de nuvem para agregados habilitados para FabricPool. Um FabricPool pode ser licenciado ou não licenciado. Quando a camada de nuvem é espelhada para outro provedor de nuvem (a camada espelhada), as duas camadas de nuvem são exibidas aqui

- Espaço total do cache

Exibe o espaço total das unidades de estado sólido (SSDs) ou unidades de alocação adicionadas a um agregado de Flash Pool. Se você ativou o Flash Pool para um agregado, mas não adicionou nenhum SSDs, o espaço de cache será exibido como 0 KB.



Esse campo será oculto se o Flash Pool estiver desativado para um agregado.

- Limites de agregado

Exibe os seguintes limites de capacidade agregada:

- Limite quase total

Especifica a porcentagem em que um agregado está quase cheio.

- Limite máximo

Especifica a porcentagem na qual um agregado está cheio.

- Limite quase comprometido

Especifica a porcentagem em que um agregado está quase sobrecarregado.

- Limite excedido

Especifica a porcentagem em que um agregado é supercomprometido.

- Outros Detalhes: Taxa de crescimento diária

Exibe o espaço em disco usado no agregado se a taxa de alteração entre as duas últimas amostras continuar por 24 horas.

Por exemplo, se um agregado usa 10 GB de espaço em disco a 2 pm e 12 GB a 6 pm, a taxa de crescimento diária (GB) para esse agregado é de 2 GB.

- Movimentação de volume

Exibe o número de operações de movimentação de volume que estão atualmente em andamento:

- Volumes para fora

Exibe o número e a capacidade dos volumes que estão sendo movidos para fora do agregado.

Você pode clicar no link para ver mais detalhes, como o nome do volume, agregado para o qual o volume é movido, o status da operação de movimentação de volume e o tempo de término estimado.

- Volumes em

Exibe o número e a capacidade restante dos volumes que estão sendo movidos para o agregado.

Você pode clicar no link para ver mais detalhes, como o nome do volume, o agregado a partir do qual o volume é movido, o status da operação de movimentação de volume e o tempo de término estimado.

- Capacidade utilizada estimada após movimentação do volume

Exibe a quantidade estimada de espaço usado (como uma porcentagem, e em KB, MB, GB e assim por diante) no agregado depois que as operações de movimentação de volume estiverem concluídas.

## • Visão geral da capacidade - volumes

Exibe gráficos que fornecem informações sobre a capacidade dos volumes contidos no agregado. É apresentada a quantidade de espaço utilizada pelo volume (capacidade utilizada) e a quantidade de espaço disponível (capacidade livre) no volume. Quando o evento espaço de volume em risco de provisionamento reduzido é gerado para volumes provisionados de forma fina, a quantidade de espaço usado pelo volume (capacidade usada) e a quantidade de espaço disponível no volume, mas não pode ser usado (capacidade inutilizável) devido a problemas de capacidade agregada é exibida.

Pode selecionar o gráfico que pretende visualizar a partir das listas pendentes. Você pode classificar os dados exibidos no gráfico para exibir detalhes como o tamanho usado, o tamanho provisionado, a capacidade disponível, a taxa de crescimento diária mais rápida e a taxa de crescimento mais lenta. Você pode filtrar os dados com base nas máquinas virtuais de armazenamento (SVMs) que contêm os volumes no agregado. Você também pode exibir detalhes de volumes provisionados de forma fina. Você pode visualizar os detalhes de pontos específicos no gráfico posicionando o cursor sobre a área de interesse. Por padrão, o gráfico exibe os 30 maiores volumes filtrados no agregado.

## **Guia informações do disco**

Exibe informações detalhadas sobre os discos no agregado selecionado, incluindo o tipo e o tamanho do RAID e o tipo de discos usados no agregado. A guia também exibe graficamente os grupos RAID e os tipos de discos usados (como SAS, ATA, FCAL, SSD ou VMDISK). Você pode ver mais informações, como o compartimento, o compartimento e a velocidade de rotação do disco, posicionando o cursor sobre os discos de paridade e os discos de dados.

### **• Dados**

Exibe graficamente detalhes sobre discos de dados dedicados, discos de dados compartilhados ou ambos. Quando os discos de dados contêm discos compartilhados, os detalhes gráficos dos discos compartilhados são exibidos. Quando os discos de dados contêm discos dedicados e discos compartilhados, os detalhes gráficos dos discos de dados dedicados e dos discos de dados compartilhados são exibidos.

#### **◦ Detalhes do RAID**

Os detalhes do RAID são exibidos apenas para discos dedicados.

- Tipo

Exibe o tipo RAID (RAID0, RAID4, RAID-DP ou RAID-TEC).

- Tamanho do grupo

Exibe o número máximo de discos permitidos no grupo RAID.

- Grupos

Exibe o número de grupos RAID no agregado.

#### **◦ Discos utilizados**

- Tipo eficaz

Exibe os tipos de discos de dados (por exemplo, ATA, SATA, FCAL, SSD ou VMDISK) no agregado.

- Discos de dados

Exibe o número e a capacidade dos discos de dados atribuídos a um agregado. Os detalhes do disco de dados não são exibidos quando o agregado contém apenas discos compartilhados.

- Discos de paridade

Exibe o número e a capacidade dos discos de paridade atribuídos a um agregado. Os detalhes do disco de paridade não são exibidos quando o agregado contém apenas discos compartilhados.

- Discos compartilhados

Exibe o número e a capacidade dos discos de dados compartilhados atribuídos a um agregado. Os detalhes do disco compartilhado são exibidos somente quando o agregado contém discos compartilhados.

- **Discos sobresselentes**

Exibe o tipo efetivo do disco, o número e a capacidade dos discos de dados sobresselentes disponíveis para o nó no agregado selecionado.



Quando um agregado é failover para o nó do parceiro, o Unified Manager não exibe todos os discos sobresselentes compatíveis com o agregado.

- **Cache SSD**

Fornecer detalhes sobre discos SSD de cache dedicados e discos SSD de cache compartilhado.

Os seguintes detalhes para os discos SSD de cache dedicados são exibidos:

- **Detalhes do RAID**

- Tipo

Exibe o tipo RAID (RAID0, RAID4, RAID-DP ou RAID-TEC).

- Tamanho do grupo

Exibe o número máximo de discos permitidos no grupo RAID.

- Grupos

Exibe o número de grupos RAID no agregado.

- **Discos utilizados**

- Tipo eficaz

Indica que os discos usados para cache no agregado são do tipo SSD.

- Discos de dados

Exibe o número e a capacidade dos discos de dados atribuídos a um agregado para cache.

- Discos de paridade

Exibe o número e a capacidade dos discos de paridade atribuídos a um agregado para cache.

- **Discos sobresselentes**

Exibe o tipo efetivo do disco, o número e a capacidade dos discos sobresselentes disponíveis para o nó no agregado selecionado para cache.



Quando um agregado é failover para o nó do parceiro, o Unified Manager não exibe todos os discos sobresselentes compatíveis com o agregado.



Fornece os seguintes detalhes para o cache compartilhado:

- **Piscina de armazenamento**

Exibe o nome do pool de armazenamento. Você pode mover o ponteiro sobre o nome do pool de armazenamento para exibir os seguintes detalhes:

- Estado

Exibe o status do pool de armazenamento, que pode estar saudável ou não saudável.

- Alocações totais

Exibe as unidades de alocação total e o tamanho no pool de armazenamento.

- Tamanho Unidade Alocação

Exibe a quantidade mínima de espaço no pool de armazenamento que pode ser alocada a um agregado.

- Discos

Exibe o número de discos usados para criar o pool de armazenamento. Se a contagem de discos na coluna do pool de armazenamento e o número de discos exibidos na guia informações do disco para esse pool de armazenamento não corresponderem, isso indica que um ou mais discos estão quebrados e o pool de armazenamento não está funcionando.

- Alocação utilizada

Exibe o número e o tamanho das unidades de alocação usadas pelos agregados. Você pode clicar no nome do agregado para exibir os detalhes do agregado.

- Alocação disponível

Exibe o número e o tamanho das unidades de alocação disponíveis para os nós. Você pode clicar no nome do nó para exibir os detalhes do agregado.

- **Cache alocado**

Exibe o tamanho das unidades de alocação usadas pelo agregado.

- **Unidades de alocação**

Exibe o número de unidades de alocação usadas pelo agregado.

- **Discos**

Exibe o número de discos contidos no pool de armazenamento.

- **Detalhes**

- Pool de storage

Exibe o número de pools de armazenamento.

- Tamanho total

Exibe o tamanho total dos pools de armazenamento.

- **Nível de nuvem**

Exibe o nome do nível de nuvem, se você tiver configurado um agregado habilitado para FabricPool, e mostra o espaço total usado. Quando a camada de nuvem é espelhada para outro fornecedor de nuvem (a camada espelhada), os detalhes das duas camadas de nuvem são exibidos aqui

### **Separador Configuration (Configuração)**

A guia Configuração exibe detalhes sobre o agregado selecionado, como seu nó de cluster, tipo de bloco, tipo de RAID, tamanho de RAID e contagem de grupo RAID:

- **Visão geral**

- **Nó**

Exibe o nome do nó que contém o agregado selecionado.

- **Tipo de bloco**

Exibe o formato de bloco do agregado: 32 bits ou 64 bits.

- **Tipo RAID**

Exibe o tipo RAID (RAID0, RAID4, RAID-DP, RAID-TEC ou RAID misto).

- **Tamanho RAID**

Exibe o tamanho do grupo RAID.

- **Grupos RAID**

Exibe o número de grupos RAID no agregado.

- **Tipo SnapLock**

Exibe o tipo de SnapLock do agregado.

- **Nível de nuvem**

Se esse for um agregado habilitado para FabricPool, os detalhes do nível de nuvem serão exibidos. Alguns campos são diferentes dependendo do provedor de armazenamento. Quando o nível de nuvem é espelhado para outro provedor de nuvem (o "nível de erro"), ambos os níveis de nuvem são exibidos aqui.

- **Fornecedor**

Exibe o nome do fornecedor de storage, por exemplo, StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud, Google Cloud Storage ou Alibaba Cloud Object Storage.

- **Nome**

Exibe o nome do nível de nuvem quando ele foi criado pelo ONTAP.

- **Servidor**

Exibe o FQDN do nível de nuvem.

- Porta

A porta que está sendo usada para se comunicar com o provedor de nuvem.

- Chave de acesso ou conta

Exibe a chave de acesso ou a conta do nível de nuvem.

- Nome do recipiente

Exibe o nome do bucket ou do contêiner do nível de nuvem.

- SSL

Exibe se a criptografia SSL está habilitada para o nível de nuvem.

### Área de história

A área Histórico exibe gráficos que fornecem informações sobre a capacidade do agregado selecionado. Além disso, você pode clicar no botão **Exportar** para criar um relatório em formato CSV para o gráfico que você está visualizando.

Você pode selecionar um tipo de gráfico na lista suspensa na parte superior do painel Histórico. Você também pode exibir detalhes de um período de tempo específico selecionando 1 semana, 1 mês ou 1 ano. Os gráficos de histórico podem ajudá-lo a identificar tendências: Por exemplo, se o uso agregado estiver constantemente violando o limite quase completo, você pode tomar a ação apropriada.

Os gráficos de histórico apresentam as seguintes informações:

- **Capacidade agregada utilizada (%)**

Exibe a capacidade usada no agregado e a tendência de como a capacidade agregada é usada com base no histórico de uso como gráficos de linha, em porcentagem, no eixo vertical (y). O período de tempo é apresentado no eixo horizontal (x). Você pode selecionar um período de tempo de uma semana, um mês ou um ano. Você pode exibir os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linha clicando na legenda apropriada. Por exemplo, quando você clica na legenda capacidade usada, a linha de gráfico capacidade usada é oculta.

- **Capacidade agregada utilizada vs capacidade total**

Exibe a tendência de como a capacidade agregada é usada com base no histórico de uso, bem como a capacidade usada e a capacidade total, como gráficos de linha, em bytes, kilobytes, megabytes, e assim por diante, no eixo vertical (y). O período de tempo é apresentado no eixo horizontal (x). Você pode selecionar um período de tempo de uma semana, um mês ou um ano. Você pode exibir os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linha clicando na legenda apropriada. Por exemplo, quando você clica na legenda capacidade de tendência usada, a linha de gráfico capacidade de tendência usada fica oculta.

- **Capacidade agregada utilizada (%) vs comprometida (%)**

Exibe a tendência de como a capacidade agregada é usada com base no histórico de uso, bem como o espaço comprometido como gráficos de linha, como uma porcentagem, no eixo vertical (y). O período de tempo é apresentado no eixo horizontal (x). Você pode selecionar um período de tempo de uma semana,

um mês ou um ano. Você pode exibir os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linha clicando na legenda apropriada. Por exemplo, quando você clica na legenda espaço comprometido, a linha de gráfico espaço comprometido fica oculta.

### **Lista de eventos**

A lista Eventos exibe detalhes sobre eventos novos e reconhecidos:

- **Gravidade**

Exibe a gravidade do evento.

- **Evento**

Exibe o nome do evento.

- **Tempo acionado**

Exibe o tempo decorrido desde que o evento foi gerado. Se o tempo decorrido exceder uma semana, o carimbo de data/hora para quando o evento foi gerado é exibido.

### **Painel dispositivos relacionados**

O painel dispositivos relacionados permite exibir o nó, os volumes e os discos do cluster relacionados ao agregado:

- **Nó**

Exibe a capacidade e o status de integridade do nó que contém o agregado. Capacidade indica a capacidade utilizável total em relação à capacidade disponível.

- **Agregados no nó**

Exibe o número e a capacidade de todos os agregados no nó de cluster que contém o agregado selecionado. O estado de saúde dos agregados também é exibido, com base no nível de gravidade mais alto. Por exemplo, se um nó de cluster contiver dez agregados, cinco dos quais exibem o status de Aviso e os cinco restantes dos quais exibem o status crítico, o status exibido será crítico.

- **Volumes**

Exibe o número e a capacidade dos volumes FlexVol e volumes FlexGroup no agregado; o número não inclui componentes FlexGroup. O estado de funcionamento dos volumes também é apresentado, com base no nível de gravidade mais elevado.

- **Pool de recursos**

Exibe os pools de recursos relacionados ao agregado.

- **Discos**

Exibe o número de discos no agregado selecionado.

### **Painel Alertas relacionados**

O painel Alertas relacionados permite exibir a lista de alertas criados para o agregado selecionado. Você também pode adicionar um alerta clicando no link Adicionar alerta ou editar um alerta existente clicando no nome do alerta.

### **Informações relacionadas**

["Visualização dos detalhes do pool de armazenamento"](#)

# Proteger e restaurar dados

## Criação, monitoramento e solução de problemas de relacionamentos de proteção

Com o Unified Manager, você cria relacionamentos de proteção, monitora e soluciona problemas de proteção espelhada e de backup de dados armazenados em clusters gerenciados, além de restaurar os dados quando substituídos ou perdidos.

### Tipos de proteção SnapMirror

Dependendo da implantação da topologia de storage de dados, o Unified Manager permite configurar vários tipos de relacionamentos de proteção SnapMirror. Todas as variações da proteção SnapMirror oferecem proteção contra recuperação de desastres com failover, mas oferecem recursos diferentes em performance, flexibilidade de versão e proteção de várias cópias de backup.

#### Relações de proteção assíncronas tradicionais da SnapMirror

A proteção assíncrona tradicional da SnapMirror fornece proteção espelhada de replicação de bloco entre volumes de origem e destino.

Nas relações SnapMirror tradicionais, as operações de espelhamento são executadas mais rápido do que em relacionamentos SnapMirror alternativos, porque a operação de espelhamento é baseada na replicação de bloco. No entanto, a proteção SnapMirror tradicional requer que o volume de destino seja executado na mesma ou posterior versão menor do software ONTAP como o volume de origem na mesma versão principal (por exemplo, versão 8.x a 8.x ou 9.x a 9.x). A replicação de uma origem 9,1 para um destino 9,0 não é suportada porque o destino está executando uma versão principal anterior.

#### Proteção assíncrona SnapMirror com replicação flexível da versão

A proteção assíncrona do SnapMirror com replicação flexível da versão fornece proteção de espelhamento de replicação lógica entre volumes de origem e destino, mesmo que esses volumes estejam sendo executados em versões diferentes do ONTAP 8,3 ou software posterior (por exemplo, versão 8,3 a 8,3.1, ou 8,3 a 9,1 ou 9.2.2 a 9,2).

Nos relacionamentos do SnapMirror com replicação flexível por versão, as operações de espelhamento não são executadas tão rapidamente quanto nas relações SnapMirror tradicionais.

Devido à execução mais lenta, o SnapMirror com proteção de replicação flexível da versão não é adequado para ser implementado em qualquer uma das seguintes circunstâncias:

- O objeto fonte contém mais de 10 milhões de arquivos para proteger.
- O objetivo do ponto de recuperação para os dados protegidos é de duas horas ou menos. (Ou seja, o destino deve sempre conter dados espelhados e recuperáveis que não são mais de duas horas mais antigos do que os dados na origem.)

Em qualquer uma das circunstâncias listadas, é necessária a execução mais rápida baseada na replicação de blocos da proteção padrão do SnapMirror.

## Proteção assíncrona SnapMirror com replicação flexível da versão e opção de backup

A proteção assíncrona do SnapMirror com a opção de replicação flexível e backup da versão oferece proteção espelhada entre os volumes de origem e destino e a funcionalidade de armazenar várias cópias dos dados espelhados no destino.

O administrador de storage pode especificar quais cópias Snapshot são espelhadas de origem para destino e também especificar por quanto tempo reter essas cópias no destino, mesmo que elas sejam excluídas na origem.

Nos relacionamentos do SnapMirror com a opção de replicação flexível de versão e backup, as operações de espelhamento não são executadas tão rapidamente como nas relações SnapMirror tradicionais.

## Replicação unificada da SnapMirror (espelhamento e cofre)

A replicação unificada do SnapMirror permite configurar a recuperação de desastres e o arquivamento no mesmo volume de destino. Assim como no SnapMirror, a proteção de dados unificada realiza uma transferência de linha de base na primeira vez que você a invoca. Uma transferência de linha de base sob a política de proteção de dados unificada padrão "MirrorAndVault" faz uma cópia Snapshot do volume de origem e, em seguida, transfere essa cópia e os blocos de dados que ela faz referência ao volume de destino. Assim como o SnapVault, a proteção de dados unificada não inclui cópias Snapshot mais antigas na linha de base.

## Proteção síncrona SnapMirror com sincronização estrita

A proteção síncrona SnapMirror com sincronização "strict" garante que os volumes primário e secundário sejam sempre uma cópia verdadeira um do outro. Se ocorrer uma falha de replicação ao tentar gravar dados no volume secundário, a e/S do cliente no volume primário será interrompida.

## Proteção síncrona SnapMirror com sincronização regular

A proteção síncrona do SnapMirror com sincronização "vehicular" não exige que o volume primário e secundário sejam sempre uma cópia verdadeira do outro, garantindo assim a disponibilidade do volume primário. Se ocorrer uma falha de replicação ao tentar gravar dados no volume secundário, os volumes primário e secundário ficam fora de sincronia e a e/S do cliente continuará para o volume primário.



O botão Restaurar e os botões de operação de relacionamento não estão disponíveis ao monitorar relações de proteção síncronas na exibição Saúde: Todos os volumes ou na página Detalhes volume / Saúde.

## Sincronização ativa do SnapMirror

O recurso de sincronização ativa do SnapMirror está disponível com o ONTAP 9.8 e posterior, e você pode usá-lo para proteger aplicações com LUNs, permitindo failover de aplicações de forma transparente, garantindo a continuidade dos negócios em caso de desastre.

Ele permite descobrir e monitorar as relações síncronas de SnapMirror para grupos de consistência (CGS) disponíveis em clusters e máquinas virtuais de armazenamento do Unified Manager. O SnapMirror active Sync é compatível com clusters AFF ou todos os clusters SAN Array (ASA), onde os clusters primário e secundário podem ser AFF ou ASA. A sincronização ativa do SnapMirror protege aplicações com LUNs iSCSI ou FCP.

Quando você visualiza os volumes e LUNs protegidos pela relação de sincronização ativa do SnapMirror, obtém uma visão unificada para relacionamentos de proteção, grupos de consistência no inventário de volumes, exibe a topologia de proteção para relacionamentos de grupo de consistência, exibe dados históricos para relacionamentos de grupo de consistência em até um ano. Você também pode baixar o

relatório. Você também pode exibir o resumo das relações de Grupo de consistência, pesquisar o suporte para relacionamentos de Grupo de consistência e obter informações sobre volumes protegidos pelo Grupo de consistência.

Na página relacionamentos, você também pode classificar, filtrar e estender a proteção nos objetos de armazenamento de origem e destino e seus relacionamentos protegidos pelo Grupo de consistência.

Para saber mais sobre a sincronização ativa do SnapMirror, "[Documentação do ONTAP 9 para sincronização ativa do SnapMirror \(anteriormente SM-BC\)](#)" consulte .

## Configuração de relacionamentos de proteção no Unified Manager

Há várias etapas que você deve executar para usar o Gerenciador Unificado e o OnCommand Workflow Automation para configurar relacionamentos do SnapMirror e do SnapVault para proteger seus dados.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você precisa ter relacionamentos de pares estabelecidos entre dois clusters ou duas máquinas virtuais de storage (SVMs).
- O OnCommand Workflow Automation precisa ser integrado ao Unified Manager:
  - "[Configure o OnCommand Workflow Automation](#)".
  - "[Verificando o armazenamento em cache da fonte de dados do Unified Manager no Workflow Automation](#)".

### Passos

1. Dependendo do tipo de relação de proteção que você deseja criar, execute um dos seguintes procedimentos:
  - "[Crie uma relação de proteção SnapMirror](#)".
  - "[Crie uma relação de proteção SnapVault](#)".
2. Se você quiser criar uma política para o relacionamento, dependendo do tipo de relacionamento que você está criando, siga um destes procedimentos:
  - "[Crie uma política do SnapVault](#)".
  - "[Crie uma política do SnapMirror](#)".
3. "[Crie uma agenda SnapMirror ou SnapVault](#)".

## Configurando uma conexão entre o Workflow Automation e o Unified Manager

Você pode configurar uma conexão segura entre o OnCommand Workflow Automation (WFA) e o Unified Manager. A conexão com o Workflow Automation permite que você use recursos de proteção, como fluxos de trabalho de configuração do SnapMirror e do SnapVault, bem como comandos para gerenciar relacionamentos do SnapMirror.

### Antes de começar

- A versão instalada do Workflow Automation deve ser 5,1.1P6 ou superior.





O "WFA pack for Management Clustered Data ONTAP" está incluído no WFA 5,1.1P6, portanto, não há necessidade de baixar este pacote da Loja de Automação NetAppStorage e instalá-lo separadamente em seu SERVIDOR WFA, como era necessário no passado.  
["Pacote WFA para gerenciar ONTAP"](#)

- Você deve ter o nome do usuário do banco de dados que criou no Unified Manager para oferecer suporte às conexões DO WFA e do Unified Manager.

Esse usuário do banco de dados deve ter sido atribuído a função de usuário do esquema de integração.

- Você deve ser atribuído a função Administrador ou a função arquiteto no Workflow Automation.
- Você deve ter o endereço do host, o número da porta 443, o nome de usuário e a senha para a configuração do Workflow Automation.
- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

### Passos

1. No painel de navegação esquerdo, clique em **Geral > Workflow Automation**.
2. Na área **Database User** da página **Workflow Automation**, selecione o nome e insira a senha do usuário do banco de dados que você criou para oferecer suporte às conexões Unified Manager e Workflow Automation.
3. Na área **credenciais de automação do fluxo de trabalho** da página, insira o nome do host ou o endereço IP (IPv4 ou IPv6) e o nome de usuário e a senha para a configuração do Workflow Automation.

Você deve usar a porta de servidor do Unified Manager (porta 443).

4. Clique em **Salvar**.
5. Se você usar um certificado autoassinado, clique em **Sim** para autorizar o certificado de segurança.

A página Workflow Automation (Automação do fluxo de trabalho) é exibida

6. Clique em **Yes** para recarregar a IU da Web e adicionar os recursos do Workflow Automation.

### Informações relacionadas

["Documentação do NetApp: OnCommand Workflow Automation \(versões atuais\)"](#)

### Verificando o armazenamento em cache da fonte de dados do Unified Manager no Workflow Automation

Você pode determinar se o armazenamento em cache da fonte de dados do Unified Manager está funcionando corretamente verificando se a aquisição da fonte de dados é bem-sucedida no Workflow Automation. Você pode fazer isso quando integrar o Workflow Automation ao Unified Manager para garantir que a funcionalidade do Workflow Automation esteja disponível após a integração.

### Antes de começar

Para executar esta tarefa, é necessário atribuir a função Administrador ou a função arquiteto no Workflow Automation.

### Passos

1. Na IU do Workflow Automation, selecione **execução > fontes de dados**.
2. Clique com o botão direito do Mouse no nome da fonte de dados do Unified Manager e selecione **adquirir agora**.
3. Verifique se a aquisição é bem-sucedida sem erros.

Erros de aquisição devem ser resolvidos para que a integração do Workflow Automation com o Unified Manager seja bem-sucedida.

## O que acontece quando o OnCommand Workflow Automation é reinstalado ou atualizado

Antes de reinstalar ou atualizar o OnCommand Workflow Automation, primeiro você deve remover a conexão entre o OnCommand Workflow Automation e o Unified Manager e garantir que todos os OnCommand Workflow Automation em execução ou tarefas agendadas estejam interrompidas.

Você também deve excluir manualmente o Unified Manager do OnCommand Workflow Automation.

Depois de reinstalar ou atualizar o OnCommand Workflow Automation, você deve configurar a conexão com o Unified Manager novamente.

## Remoção da configuração do OnCommand Workflow Automation do Gerenciador Unificado

Você pode remover a configuração do OnCommand Workflow Automation do Unified Manager quando não quiser mais usar o Workflow Automation.

### Antes de começar

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

### Passos

1. No painel de navegação à esquerda, clique em **Geral > Workflow Automation** no menu Configuração à esquerda.
2. Na página **Workflow Automation**, clique em **Remove Setup** (Remover configuração).

## Execução de failover e failback de uma relação de proteção

Quando um volume de origem em sua relação de proteção é desativado devido a uma falha de hardware ou a um desastre, você pode usar os recursos de relação de proteção no Unified Manager para tornar o destino de proteção leitura/gravação acessível e fazer failover para esse volume até que a origem esteja on-line novamente. Em seguida, você pode retornar à fonte original quando ela estiver disponível para fornecer dados.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Tem de ter configurado o OnCommand Workflow Automation para executar esta operação.

### Passos

1. "[Quebre a relação SnapMirror](#)".

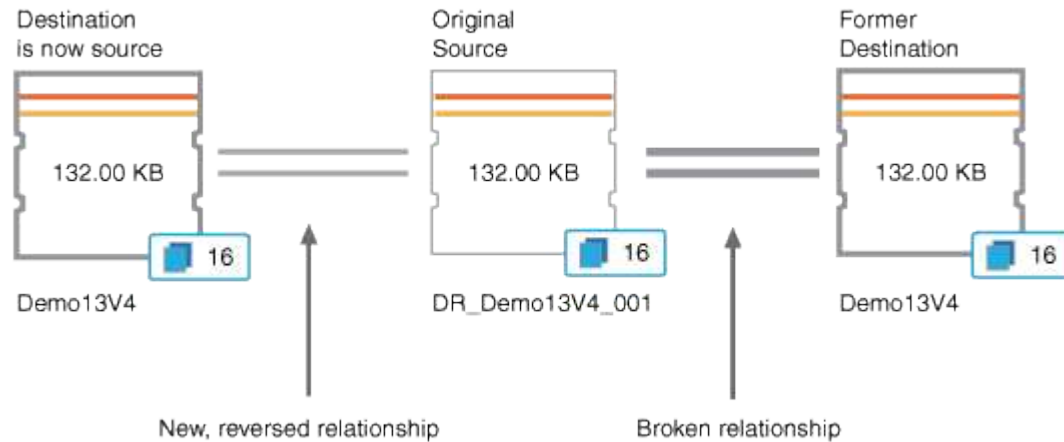
É necessário interromper o relacionamento antes de converter o destino de um volume de proteção de

dados em um volume de leitura/gravação e antes de reverter o relacionamento.

## 2. "Inverta a relação de proteção".

Quando o volume de origem original estiver novamente disponível, você poderá decidir restabelecer a relação de proteção original restaurando o volume de origem. Antes de restaurar a origem, é necessário sincronizá-la com os dados gravados no destino anterior. Use a operação de resincronização reversa para criar uma nova relação de proteção invertendo as funções da relação original e sincronizando o volume de origem com o destino anterior. Uma nova cópia Snapshot da linha de base é criada para o novo relacionamento.

A relação invertida é semelhante a uma relação em cascata:



## 3. "Quebre a relação revertida do SnapMirror".

Quando o volume de origem original for resincronizado e puder servir novamente os dados, use a operação de quebra para quebrar a relação invertida.

## 4. "Remova a relação".

Quando o relacionamento invertido não for mais necessário, você deve remover esse relacionamento antes de restabelecer o relacionamento original.

## 5. "Ressincronizar o relacionamento".

Use a operação de resincronização para sincronizar dados da origem para o destino e restabelecer a relação original.

### Quebrar uma relação de SnapMirror a partir da página de detalhes de volume / Saúde

Você pode quebrar uma relação de proteção da página de detalhes de volume / Saúde e interromper as transferências de dados entre um volume de origem e destino em uma relação do SnapMirror. Você pode interromper um relacionamento quando quiser migrar dados, para recuperação de desastres ou para teste de aplicações. O volume de destino é alterado para um volume de leitura e gravação. Você não pode quebrar um relacionamento SnapVault.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

### Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, selecione na topologia a relação do SnapMirror que deseja quebrar.
2. Clique com o botão direito do rato no destino e selecione **Break** no menu.

É apresentada a caixa de diálogo Break Relationship (interromper relação).

3. Clique em **continuar** para quebrar o relacionamento.
4. Na topologia, verifique se o relacionamento está quebrado.

### Reverter relações de proteção a partir da página de detalhes de volume / Saúde

Quando um desastre desativa o volume de origem em sua relação de proteção, você pode usar o volume de destino para servir dados convertendo-os para leitura/gravação enquanto você reparar ou substituir a origem. Quando a origem estiver novamente disponível para receber dados, você poderá usar a operação de resincronização reversa para estabelecer a relação na direção inversa, sincronizando os dados na origem com os dados no destino de leitura/gravação.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.
- O relacionamento não deve ser um relacionamento SnapVault.
- Uma relação de proteção já deve existir.
- A relação de proteção deve ser quebrada.
- Tanto a origem como o destino devem estar online.
- A origem não deve ser o destino de outro volume de proteção de dados.
- Quando você executa essa tarefa, os dados na fonte mais recente do que os dados na cópia Snapshot comum são excluídos.
- As políticas e os horários criados na relação de resincronização reversa são os mesmos que os da relação de proteção original.

Se as políticas e agendas não existirem, elas são criadas.

### Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, localize na topologia a relação SnapMirror na qual você deseja reverter a origem e o destino e clique com o botão direito do Mouse nela.
2. Selecione **Reverse Resync** no menu.

A caixa de diálogo Reverse Resync (Reverse Resync) é exibida.

3. Verifique se a relação exibida na caixa de diálogo **Reverse Resync** é aquela para a qual você deseja executar a operação de resincronização reversa e clique em **Submit**.

A caixa de diálogo Reverse Resync (Reverse Resync) é fechada e um link de tarefa é exibido na parte superior da página volume / Health details (Detalhes de volume / Saúde).

4. **Opcional:** clique em **Exibir trabalhos** na página de detalhes **volume / Saúde** para rastrear o status de cada trabalho de resincronização reversa.

É apresentada uma lista filtrada de trabalhos.

5. **Opcional:** clique na seta **voltar** no seu navegador para retornar à página de detalhes **volume / Saúde**.

A operação de resincronização reversa é concluída quando todas as tarefas de trabalho são concluídas com êxito.

## Remover uma relação de proteção da página de detalhes de volume / Saúde

Você pode remover uma relação de proteção para excluir permanentemente uma relação existente entre a origem e o destino selecionados: Por exemplo, quando você deseja criar uma relação usando um destino diferente. Esta operação remove todos os metadados e não pode ser desfeita.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

### Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, selecione na topologia a relação SnapMirror que deseja remover.
2. Clique com o botão direito do rato no nome do destino e selecione **Remover** no menu.

A caixa de diálogo Remover relacionamento é exibida.

3. Clique em **continuar** para remover o relacionamento.

A relação é removida da página de detalhes de volume / Saúde.

## Ressincronizar relações de proteção a partir da página de detalhes de volume / Saúde

É possível ressincronizar dados em um relacionamento SnapMirror ou SnapVault que foi quebrado e, em seguida, o destino foi feito leitura/gravação para que os dados na origem correspondam aos dados no destino. Você também pode ressincronizar quando uma cópia Snapshot comum necessária no volume de origem for excluída, causando falha nas atualizações do SnapMirror ou do SnapVault.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Tem de ter configurado o OnCommand Workflow Automation.

### Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, localize na topologia a relação de proteção que você deseja ressincronizar e clique com o botão direito do Mouse nela.

2. Selecione **Resynchronize** no menu.

Alternativamente, no menu **ações**, selecione **relacionamento** > **Resincronizar** para resincronizar a relação para a qual você está visualizando os detalhes no momento.

A caixa de diálogo Resincronizar é exibida.

3. Na guia **Opções de resincronização**, selecione uma prioridade de transferência e a taxa de transferência máxima.

4. Clique em **cópias snapshot de origem**; em seguida, na coluna **cópia Snapshot**, clique em **predefinição**.

A caixa de diálogo Selecionar cópia Snapshot de origem é exibida.

5. Se você quiser especificar uma cópia Snapshot existente em vez de transferir a cópia Snapshot padrão, clique em **cópia Snapshot existente** e selecione uma cópia Snapshot na lista.

6. Clique em **Enviar**.

Você será retornado à caixa de diálogo Resincronizar.

7. Se você selecionou mais de uma fonte para resincronizar, clique em **Default** para a próxima fonte para a qual deseja especificar uma cópia Snapshot existente.

8. Clique em **Enviar** para iniciar o trabalho de resincronização.

O trabalho de resincronização é iniciado, você é retornado à página de detalhes de volume / Saúde e um link trabalhos é exibido na parte superior da página.

9. **Opcional:** clique em **Exibir trabalhos** na página **Detalhes de volume / Saúde** para acompanhar o status de cada trabalho de resincronização.

É apresentada uma lista filtrada de trabalhos.

10. **Opcional:** clique na seta **voltar** no seu navegador para retornar à página de detalhes **volume / Saúde**.

O trabalho de resincronização é concluído quando todas as tarefas de trabalho forem concluídas com êxito.

## Resolução de uma falha de trabalho de proteção

Esse fluxo de trabalho fornece um exemplo de como você pode identificar e resolver uma falha de tarefa de proteção no painel do Unified Manager.

### Antes de começar

Como algumas tarefas nesse fluxo de trabalho exigem que você faça login usando a função Administrador, você deve estar familiarizado com as funções necessárias para usar várias funcionalidades.

Nesse cenário, você acessa a página Painel para ver se há algum problema com seus trabalhos de proteção. Na área Incidente de proteção, você percebe que há um incidente de trabalho terminado, mostrando um erro Falha no trabalho de proteção em um volume. Investigue este erro para determinar a possível causa e a possível resolução.

### Passos

1. No painel incidentes de proteção da área incidentes e riscos não resolvidos do Painel, clique no evento

## Falha no trabalho de proteção.



O texto vinculado para o evento é escrito no formulário `object_name:/object_name - Error Name`, como `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

A página de detalhes do evento para o trabalho de proteção com falha é exibida.

2. Reveja a mensagem de erro no campo causa da área **Summary** para determinar o problema e avaliar potenciais ações corretivas.

["Identificar o problema e executar ações corretivas para um trabalho de proteção com falha"](#) Consulte .

### Identificar o problema e executar ações corretivas para um trabalho de proteção com falha

Você analisa a mensagem de erro de falha do trabalho no campo causa na página de detalhes do evento e determina que o trabalho falhou devido a um erro de cópia Snapshot. Em seguida, avance para a página de detalhes de volume / Saúde para obter mais informações.

#### Antes de começar

Tem de ter a função Administrador de aplicações.

A mensagem de erro fornecida no campo causa na página de detalhes do evento contém o seguinte texto sobre o trabalho com falha:

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

Esta mensagem fornece as seguintes informações:

- Um trabalho de cópia de segurança ou espelho não foi concluído com êxito.

A tarefa envolveu uma relação de proteção entre o volume de origem `cluster2_src_vol2` no servidor virtual `cluster2_src_svm` e o volume de destino `managed_svc2_vol3` no servidor virtual chamado `cluster3_dst_svm`.

- Um trabalho de cópia Snapshot falhou para o `0426cluster2_src_vol2snap` volume de origem `cluster2_src_svm:/cluster2_src_vol2`.

Nesse cenário, você pode identificar a causa e as possíveis ações corretivas da falha do trabalho. No entanto, a resolução da falha requer que você acesse a IU da Web do Gerenciador do sistema ou os comandos da CLI do ONTAP.

#### Passos

1. Você analisa a mensagem de erro e determina que uma tarefa de cópia Snapshot falhou no volume de origem, indicando que provavelmente há um problema com o volume de origem.

Opcionalmente, você pode clicar no link **Detalhes da tarefa** no final da mensagem de erro, mas para os fins deste cenário, você escolhe não fazer isso.

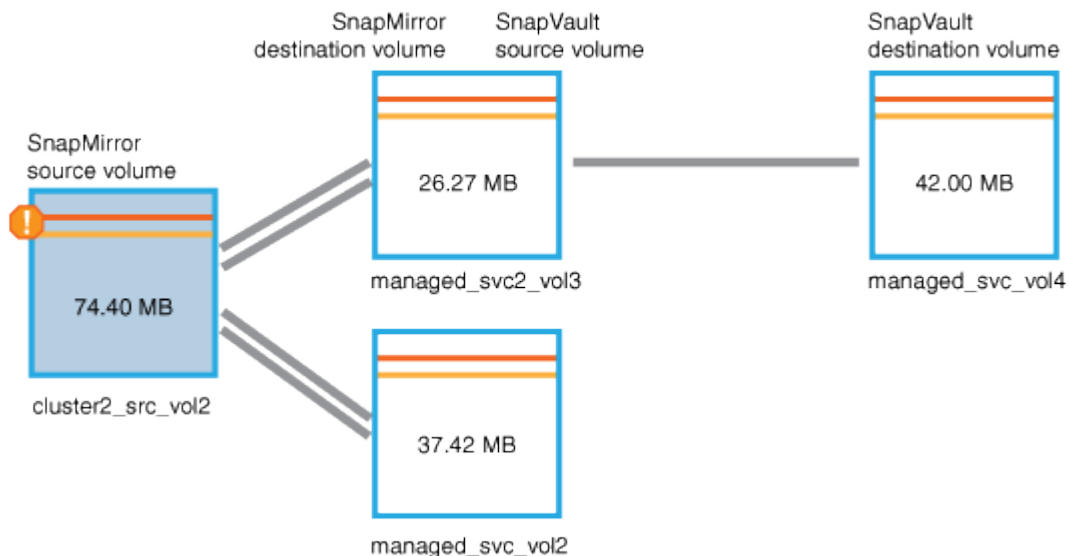
2. Você decide que deseja tentar resolver o evento, para fazer o seguinte:
  - a. Clique no botão **Assign to** e selecione **me** no menu.
  - b. Clique no botão **confirmar** para que você não continue a receber notificações de alerta repetidas, se os alertas tiverem sido definidos para o evento.
  - c. Opcionalmente, você também pode adicionar notas sobre o evento.
3. Clique no campo **fonte** no painel **Resumo** para ver detalhes sobre o volume de origem.

O campo **Source** contém o nome do objeto de origem: Neste caso, o volume no qual o trabalho de cópia Snapshot foi agendado.

A página de detalhes de volume / Saúde é exibida para `cluster2_src_vol2`, mostrando o conteúdo da guia proteção.

4. Olhando para o gráfico de topologia de proteção, você vê um ícone de erro associado ao primeiro volume na topologia, que é o volume de origem da relação SnapMirror.

Você também vê as barras horizontais no ícone de volume de origem, indicando os limites de aviso e erro definidos para esse volume.



5. Coloque o cursor sobre o ícone de erro para ver a caixa de diálogo pop-up que exibe as configurações de limite e ver que o volume excedeu o limite de erro, indicando um problema de capacidade.
6. Clique na guia **capacidade**.

Informações sobre a capacidade sobre as exibições de volume `cluster2_src_vol2`.

7. No painel **Capacity**, você vê que há um ícone de erro no gráfico de barras, indicando novamente que a capacidade do volume ultrapassou o nível de limite definido para o volume.
8. Abaixo do gráfico de capacidade, você vê que o crescimento automático de volume foi desativado e que uma garantia de espaço de volume foi definida.



Você pode decidir ativar o crescimento automático, mas para os fins desse cenário, você decide investigar mais antes de tomar uma decisão sobre como resolver o problema de capacidade.

9. Role para baixo até a lista **Eventos** e veja que os eventos Falha no trabalho de proteção, dias de volume até cheio e espaço de volume cheio foram gerados.
10. Na lista **Eventos**, você clica no evento **espaço em volume completo** para obter mais informações, tendo decidido que esse evento parece mais relevante para o seu problema de capacidade.

A página Detalhes do evento exibe o evento espaço de volume completo para o volume de origem.

11. Na área **Resumo**, você lê o campo causa do evento: `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Abaixo da área Resumo, você verá ações corretivas sugeridas.



As ações corretivas sugeridas são exibidas apenas para alguns eventos, para que você não veja essa área para todos os tipos de eventos.

Você clica na lista de ações sugeridas que você pode executar para resolver o evento espaço de volume cheio:

- Ative o crescimento automático neste volume.
  - Redimensione o volume.
  - Habilite e execute a deduplicação nesse volume.
  - Ative e execute a compactação neste volume.
13. Você decide ativar o crescimento automático no volume, mas para isso, você deve determinar o espaço livre disponível no agregado pai e a taxa de crescimento do volume atual:
    - a. Observe o agregado pai, `cluster2_src_aggr1`, no painel **Related Devices** (dispositivos relacionados).



Você pode clicar no nome do agregado para obter mais detalhes sobre o agregado.

Você determina que o agregado tem espaço suficiente para ativar o volume com crescimento automático.

- b. Na parte superior da página, olhe para o ícone que indica um incidente crítico e reveja o texto abaixo do ícone.

Você determina que "dias completos: Menos de um dia | taxa de crescimento diária: 5,4%".

14. Vá para o Gerenciador do sistema ou acesse a CLI do ONTAP para ativar a `volume autogrow` opção.



Anote os nomes do volume e do agregado para que você os tenha disponíveis ao ativar o crescimento automático.

15. Depois de resolver o problema de capacidade, retorne à página de detalhes do **evento** do Unified Manager e marque o evento como resolvido.

## Resolvendo problemas de atraso

Este fluxo de trabalho fornece um exemplo de como você pode resolver um problema de atraso. Nesse cenário, você é um administrador ou operador acessando a página do Unified Manager Dashboard para ver se há algum problema com seus relacionamentos de proteção e, se existirem, para encontrar soluções.

### Antes de começar

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

Na página Painel, você analisa a área incidentes e riscos não resolvidos e vê um erro de atraso do SnapMirror no painel proteção em riscos de proteção.

### Passos

1. No painel **proteção** na página **Painel**, localize o erro de atraso de relacionamento do SnapMirror e clique nele.

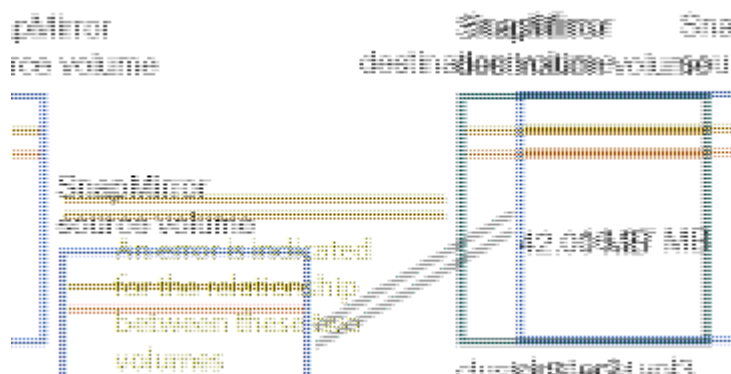
A página de detalhes do evento para o evento de erro de atraso é exibida.

2. Na página de detalhes do **evento**, você pode executar uma ou mais das seguintes tarefas:
  - Revise a mensagem de erro no campo causa da área Resumo para determinar se há alguma ação corretiva sugerida.
  - Clique no nome do objeto, neste caso um volume, no campo origem da área Resumo para obter detalhes sobre o volume.
  - Procure por notas que possam ter sido adicionadas sobre este evento.
  - Adicione uma nota ao evento.
  - Atribua o evento a um usuário específico.
  - Confirmar ou resolver o evento.
3. Nesse cenário, você clica no nome do objeto (neste caso, um volume) no campo fonte da área **Resumo** para obter detalhes sobre o volume.

É apresentado o separador proteção da página volume / Health details (Detalhes do volume / Saúde).

4. Na guia **proteção**, você vê o diagrama de topologia.

Observe que o volume com o erro de atraso é o último volume em uma cascata SnapMirror de três volumes. O volume selecionado é delineado em cinza escuro e uma linha laranja dupla do volume de origem indica um erro de relacionamento SnapMirror.



5. Clique em cada um dos volumes na cascata SnapMirror.

À medida que seleciona cada volume, as informações de proteção nas áreas Resumo, topologia, Histórico, Eventos, dispositivos relacionados e Alertas relacionados mudam para exibir detalhes relevantes para o volume selecionado.

6. Você olha para a área **Summary** e posiciona o cursor sobre o ícone de informações no campo **Update Schedule** para cada volume.

Nesse cenário, você nota que a política SnapMirror é DPDefault, e a programação do SnapMirror é atualizada de hora em hora em cinco minutos após a hora. Você percebe que todos os volumes no relacionamento estão tentando concluir uma transferência SnapMirror ao mesmo tempo.

7. Para resolver o problema de atraso, você modifica as programações de dois volumes em cascata para que cada destino inicie uma transferência de SnapMirror depois que sua origem concluir uma transferência.

## Gerenciamento e monitoramento de relações de proteção

Com o Active IQ Unified Manager, você cria relacionamentos de proteção, monitora e soluciona problemas de relacionamentos SnapMirror e SnapVault em clusters gerenciados e restaura dados quando eles são sobrescritos ou perdidos.

Para operações do SnapMirror, existem dois tipos de replicação:

- Assíncrono

A replicação do volume primário para o volume secundário é determinada por um agendamento.

- Síncrono

A replicação é realizada simultaneamente no volume primário e secundário.

Você pode executar até 10 tarefas de proteção simultaneamente sem impacto no desempenho. Você pode ter algum impactos no desempenho ao executar entre 11 e 30 tarefas simultaneamente. A execução de mais de 30 trabalhos em simultâneo não é recomendada.

### Visualização do estado da proteção do volume

A página proteção de dados apresenta uma visão holística dos detalhes de proteção de dados para todos os volumes protegidos em um único cluster ou todos os clusters em um data center.

#### Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Dependendo se você deseja exibir o status de proteção de dados para todos os clusters monitorados ou para um único cluster, selecione **todos os clusters** ou selecione um único cluster no menu suspenso.
3. Clique na seta para a direita na parte superior do painel proteção de dados. A página **proteção de dados** é exibida.

Dependendo se você selecionou um único ou todos os clusters no data center, essa página exibe o status de

proteção de dados dos volumes protegidos por cópias Snapshot ou políticas SnapMirror, além de exibir a contagem de volumes não protegidos.

A seleção de um cluster na lista **Cluster individual** exibe o status de proteção de snapshot e relação SnapMirror dos volumes protegidos nesse cluster.

Clicar nos eventos desta página leva-o à página de detalhes do evento. Você pode clicar no link **Exibir tudo** para exibir todos os eventos de proteção ativa na página de inventário do Gerenciamento de Eventos. Você pode passar o Mouse para ver as respectivas contagens e legendas. Você pode clicar em:

- Os gráficos de barras de volumes e volumes não protegidos por cópias Snapshot para acessar a página volumes e visualizar os detalhes.
- Os gráficos de barras para todas as relações vão para a página relacionamentos, onde os detalhes são filtrados pelo cluster de origem.

### Ver o status de proteção de volumes protegidos por cópias Snapshot

**Visão geral das cópias Snapshot:** Uma visão geral dos volumes protegidos por cópias Snapshot, como:

- O número total de volumes protegidos e não protegidos por cópias Snapshot.
- O número total de volumes que estão usando ou excedendo o espaço de reserva para as cópias Snapshot.

**Snapshot Copies Analysis** detalha as seguintes informações:

- Eventos individuais para cópias Snapshot, incluindo os eventos levantados nas últimas 24 horas.
- Gráfico detalhado para volumes protegidos e não protegidos por cópias Snapshot.
- Volumes que usam, não estão usando, e em violação da capacidade de cópia Snapshot reservada.
- A separação do volume conta em termos do número de cópias Snapshot.

### Pontos a observar para cópias Snapshot

- Para contar os volumes protegidos por cópias Snapshot, os volumes de origem e destino são considerados.
- O número de cópias Snapshot devolvidas destina-se apenas aos volumes on-line e disponíveis.
- O intervalo de gráfico para o número de cópias Snapshot é dinâmico. Ele é gerado com base no número de instantâneos presentes no cluster selecionado.
- Para considerar um volume como protegido, a programação da cópia Snapshot do volume deve estar ativada.
- O valor do espaço de reserva para cópias Snapshot é importante para visualizar a quantidade de espaço em disco utilizada ou para calcular o espaço que pode ser recuperado se uma ou mais cópias snapshot forem excluídas.

### Exibir status de proteção para relacionamentos do SnapMirror


**Visão geral do SnapMirror:** Uma visão geral dos volumes protegidos pelas políticas do SnapMirror, como:

- Número de volumes protegidos pelas respectivas políticas de SnapMirror, como relacionamentos de volume SnapMirror, recuperação de desastres de VM de storage (SVM-DR) e suas combinações.
- O número total de relacionamentos do SnapMirror que apresentam atraso no objetivo do ponto de

restauração (RPO) com base no status de atraso.

**Análise SnapMirror** detalha as seguintes informações:

- Eventos individuais criados para as relações SnapMirror, incluindo os eventos levantados nas últimas 24 horas
- O número de volumes protegidos por cada tipo de política do SnapMirror.
- O número de relacionamentos protegidos pelos tipos de relacionamento do SnapMirror, como espelhamento assíncrono, cofre assíncrono, espelhamento assíncrono, StricxSync, grupo de consistência de sincronização ativa do SnapMirror e sincronização.
- O número de relacionamentos saudáveis e não saudáveis.
- Separação da contagem da relação de volume. Você pode alternar os gráficos por tempo e status de atraso do RPO.

• Limites de atraso para relacionamento não gerenciado. Pode clicar no ícone de definições (  ) para configurar as definições de limite de atraso. Para obter mais informações, ["Configuração de configurações de limite de atraso para relacionamentos de proteção não gerenciados"](#) consulte .

**Pontos a serem observados para relacionamentos SnapMirror**

- Para contagem de relações SnapMirror, os volumes de origem, que são ativados para leitura e escrita, são contados. Os volumes de destino e raiz não são considerados.
- Para a relação SnapMirror, os eventos são exibidos para o cluster de origem.
- A contagem de relacionamentos do SnapMirror inclui o número de volumes com fontes e destinos nos mesmos clusters ou diferentes.
- A duração de atraso do atraso RPO na replicação de dados baseia-se na relação SnapMirror. O status é categorizado como `ok`, `warning`, ou `error`, com base no limite de relacionamento definido. Você pode olhar para o status para determinar se os parâmetros estão funcionando como esperado, ou se você precisa resolver qualquer problema.
- Se um volume tiver vários relacionamentos SnapMirror, cada tipo de relacionamento será contado para o atraso RPO.
- As relações de volume são consideradas não saudáveis se houver problemas na replicação de dados entre a origem e o destino, por exemplo, quando a relação é interrompida.

**Visualize clusters protegidos pela configuração do MetroCluster**

O painel **proteção MetroCluster** na página **proteção de dados** exibe o número de clusters protegidos ou não pela configuração MetroCluster em FC ou IP no seu site. Clicar nos gráficos de barras neste painel leva você à página clusters onde os detalhes do cluster são filtrados com base nos clusters protegidos ou desprotegidos. Para obter informações sobre como monitorar a configuração do MetroCluster, ["Monitoramento de configurações do MetroCluster"](#) consulte .

**Exibindo relações de proteção de volume**

Na visualização relacionamento: Todas as relações e na página relacionamentos de volume, você pode exibir o status das relações SnapMirror e SnapVault de volume existentes. Você também pode examinar detalhes sobre relacionamentos de proteção, incluindo status de transferência e atraso, detalhes de origem e destino, informações de programação e política, etc.

## Antes de começar

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

Você também pode iniciar comandos de relacionamento a partir desta página.

## Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **relacionamento > todos os relacionamentos**.

A visualização relacionamento: Todas as relações é exibida.

3. Escolha uma das seguintes formas de visualizar os detalhes de proteção de volume:
  - Para exibir informações atuais sobre todas as relações de volume, permaneça na página padrão **todas as relações**.
  - Para exibir informações detalhadas sobre as tendências de transferência de volume durante um período de tempo, no menu Exibir, selecione relação: Exibição Status da transferência de 1 meses.
  - Para ver informações detalhadas sobre a atividade de transferência de volume dia a dia, no menu Ver, selecione relação: Visualização da taxa de transferência de 1 meses.



As exibições de transferência de volume exibem informações somente para volumes em relacionamentos assíncronos - volumes em relacionamentos síncronos não são exibidos.

## Monitoramento de LUNs em uma relação de Grupo de consistência

Se o seu ambiente ONTAP oferecer suporte à sincronização ativa do SnapMirror para proteger aplicativos com LUNs, você poderá visualizar e monitorar esses LUNs no Active IQ Unified Manager.

A sincronização ativa do SnapMirror garante o objetivo de tempo de recuperação zero (rto) durante o failover em ambientes SAN. Em uma implantação típica com suporte à sincronização ativa do SnapMirror, os LUNs nos volumes são protegidos por relacionamentos de grupo de consistência.

Esses LUNs primários e secundários são LUNs compostos ou um par de LUNs de réplica com o mesmo UUID e número de série. As operações de e/S (leitura e gravação) são multiplexadas nos locais de origem e destino nesses LUNs compostos, garantindo transparência.

Para visualizar LUNs compostos, os clusters primário e secundário com os LUNs que fazem parte da relação de Grupo de consistência devem ser adicionados e descobertos no Unified Manager. Apenas iSCSI e FCP são suportados.

Para obter informações sobre a sincronização ativa do SnapMirror, "[Documentação do ONTAP 9 para sincronização ativa do SnapMirror \(anteriormente SM-BC\)](#)" consulte .

Para exibir LUNs compostos em seu ambiente, siga estas etapas:

## Passos

1. No painel de navegação esquerdo, clique em **Storage > LUNs**.
2. No menu Exibir, selecione **relacionamento > todos os LUNs**.

A relação: É apresentada a vista de todos os LUNs.

Você pode exibir os detalhes do LUN, como o nome do LUN, o volume, a VM de armazenamento que hospeda o LUN, o cluster, o Grupo de consistência e o LUN do parceiro. Você pode clicar em cada um desses componentes para detalhar uma visualização detalhada. Clicar no Grupo de consistência leva você para a página de relacionamentos.

Clicar no LUN do parceiro permite visualizar os detalhes de configuração na guia SAN da página Detalhes da VM de armazenamento da VM na qual o LUN do parceiro está hospedado. São apresentadas informações como os iniciadores e grupos de iniciadores e outros aspectos do LUN do parceiro.

Você pode executar as funções de nível de grade padrão de classificação, filtragem, geração e upload de relatórios para os LUNs protegidos em seu ambiente.

## **Criando uma relação de proteção SnapVault a partir da visualização integridade: Todos os volumes**

Você pode usar a visualização integridade: Todos os volumes para criar relacionamentos do SnapVault para um ou mais volumes na mesma VM de storage, a fim de habilitar backups de dados para fins de proteção.

### **Antes de começar**

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

O menu **Protect** não é exibido nas seguintes instâncias:

- Se as configurações RBAC não permitirem essa ação: Por exemplo, se você tiver apenas Privileges de operador
- Quando o ID do volume é desconhecido: Por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

### **Passos**

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. Na exibição **Saúde: Todos os volumes**, selecione um volume que você deseja proteger e clique em **proteger**.

Como alternativa, para criar vários relacionamentos de proteção na mesma máquina virtual de armazenamento (SVM), selecione um ou mais volumes na exibição Saúde: Todos os volumes e clique em **proteger** na barra de ferramentas.

3. Selecione **SnapVault** no menu.

A caixa de diálogo Configurar proteção é iniciada.

4. Clique em **SnapVault** para exibir a guia **SnapVault** e configurar as informações de volume secundário.
5. Clique em **Avançado** para definir a exclusão de dados duplicados, compactação, crescimento automático e garantia de espaço, conforme necessário, e clique em **aplicar**.
6. Preencha a área **informações de destino** e a área **Configurações de relacionamento** na guia **SnapVault**.
7. Clique em **aplicar**.

Você retorna à exibição Saúde: Todos os volumes.

8. Clique no link trabalho de configuração de proteção na parte superior da exibição **Saúde: Todos os volumes**.

Se estiver a criar apenas uma relação de proteção, é apresentada a página Detalhes do trabalho; no entanto, se estiver a criar mais do que uma relação de proteção, é apresentada uma lista filtrada de todos os trabalhos associados à operação de proteção.

9. Execute um dos seguintes procedimentos:

- Se tiver apenas um trabalho, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído.
- Se tiver mais de um trabalho:
  - i. Clique num trabalho na lista de trabalhos.
  - ii. Clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído.
  - iii. Use o botão **voltar** para retornar à lista filtrada e exibir outro trabalho.

## **Criar uma relação de proteção SnapVault a partir da página de detalhes de volume / Saúde**

Você pode criar uma relação do SnapVault usando a página de detalhes de volume / integridade para que os backups de dados sejam ativados para fins de proteção em volumes.

### **Antes de começar**

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation para executar esta tarefa.

O menu **Protect** não é exibido nas seguintes instâncias:

- Se as configurações RBAC não permitirem essa ação: Por exemplo, se você tiver apenas Privileges de operador
- Quando o ID do volume é desconhecido: Por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

### **Passos**

1. Na guia **proteção** da página de detalhes **volume / Saúde**, clique com o botão direito do Mouse em um volume na exibição de topologia que você deseja proteger.
2. Selecione **Protect > SnapVault** no menu.

A caixa de diálogo Configurar proteção é iniciada.

3. Clique em **SnapVault** para exibir a guia **SnapVault** e configurar as informações de recursos secundários.
4. Clique em **Avançado** para definir a exclusão de dados duplicados, compactação, crescimento automático e garantia de espaço, conforme necessário, e clique em **aplicar**.
5. Preencha a área **informações de destino** e a área **Configurações de relacionamento** na caixa de diálogo **Configurar proteção**.
6. Clique em **aplicar**.



Regressa à página de detalhes de volume / Saúde.

7. Clique no link do trabalho de configuração de proteção na parte superior da página de detalhes **volume / Saúde**.

É apresentada a página Detalhes do trabalho.

8. Clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído.

Quando as tarefas da tarefa estiverem concluídas, as novas relações são apresentadas na vista de topologia da página volume / Health details (Detalhes do volume / Saúde).

## **Criando uma relação de proteção SnapMirror a partir da visualização integridade: Todos os volumes**

Usando a exibição integridade: Todos os volumes, você pode criar vários relacionamentos de proteção SnapMirror ao mesmo tempo, selecionando mais de um volume na mesma VM de storage.

### **Antes de começar**

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

O menu **Protect** não é exibido nas seguintes instâncias:

- Se as configurações RBAC não permitirem essa ação: Por exemplo, se você tiver apenas Privileges de operador
- Quando o ID do volume é desconhecido: Por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

### **Passos**

1. Na exibição **Saúde: Todos os volumes**, selecione um volume que você deseja proteger.

Como alternativa, para criar vários relacionamentos de proteção no mesmo SVM, selecione um ou mais volumes na exibição Saúde: Todos os volumes e clique em **proteger > SnapMirror** na barra de ferramentas.

A caixa de diálogo Configurar proteção é exibida.

2. Clique em **SnapMirror** para visualizar a guia **SnapMirror** e configurar as informações de destino.
3. Clique em **Avançado** para definir a garantia de espaço, conforme necessário, e clique em **aplicar**.
4. Preencha a área **informações de destino** e a área **Configurações de relacionamento** na guia **SnapMirror**.
5. Clique em **aplicar**.

Você retorna à exibição Saúde: Todos os volumes.

6. Clique no link trabalho de configuração de proteção na parte superior da exibição **Saúde: Todos os volumes**.

Se estiver a criar apenas uma relação de proteção, é apresentada a página Detalhes do trabalho; no entanto, se estiver a criar mais do que uma relação de proteção, é apresentada uma lista de todos os trabalhos associados à operação de proteção.

#### 7. Execute um dos seguintes procedimentos:

- Se tiver apenas um trabalho, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído.
- Se tiver mais de um trabalho:
  - i. Clique num trabalho na lista de trabalhos.
  - ii. Clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído.
  - iii. Use o botão **voltar** para retornar à lista filtrada e exibir outro trabalho.

Dependendo do SVM de destino especificado durante a configuração ou das opções habilitadas nas configurações avançadas, a relação SnapMirror resultante pode ser uma das várias variações possíveis:

- Se você especificou um SVM de destino que seja executado na mesma ou em uma versão mais recente do ONTAP em comparação com a do volume de origem, uma relação do SnapMirror baseada em replicação de bloco será o resultado padrão.
- Se você especificou um SVM de destino que seja executado na mesma ou em uma versão mais recente do ONTAP em comparação com a do volume de origem, mas ativou a replicação flexível de versão nas configurações avançadas, o resultado será uma relação do SnapMirror com a replicação flexível de versão.
- Se você especificou um SVM de destino que é executado em uma versão anterior do ONTAP do que a do volume de origem e a versão anterior dá suporte à replicação flexível de versão, uma relação do SnapMirror com a replicação flexível de versão será o resultado automático.

## **Criar uma relação de proteção SnapMirror a partir da página de detalhes de volume / Saúde**

Você pode usar a página de detalhes de volume / integridade para criar uma relação do SnapMirror para que a replicação de dados seja ativada para fins de proteção. A replicação do SnapMirror permite restaurar dados do volume de destino em caso de perda de dados na origem.

### **Antes de começar**

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

O menu **Protect** não é exibido nas seguintes instâncias:

- Se as configurações RBAC não permitirem essa ação: Por exemplo, se você tiver apenas Privileges de operador
- Quando o ID do volume é desconhecido: Por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

Você pode executar até 10 tarefas de proteção simultaneamente sem impacto no desempenho. Você pode ter algum impactos no desempenho ao executar entre 11 e 30 tarefas simultaneamente. A execução de mais de

30 trabalhos em simultâneo não é recomendada.

## Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, clique com o botão direito do Mouse na exibição de topologia o nome de um volume que você deseja proteger.
2. Selecione **Protect > SnapMirror** no menu.

A caixa de diálogo Configurar proteção é exibida.

3. Clique em **SnapMirror** para visualizar a guia **SnapMirror** e configurar as informações de destino.
4. Clique em **Avançado** para definir a garantia de espaço, conforme necessário, e clique em **aplicar**.
5. Preencha a área **informações de destino** e a área **Configurações de relacionamento** na caixa de diálogo **Configurar proteção**.
6. Clique em **aplicar**.

Regressa à página de detalhes de volume / Saúde.

7. Clique no link do trabalho de configuração de proteção na parte superior da página de detalhes **volume / Saúde**.

As tarefas e os detalhes do trabalho são apresentados na página Detalhes do trabalho.

8. Na página de detalhes do **trabalho**, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído.
9. Quando as tarefas de trabalho estiverem concluídas, clique em **voltar** no seu navegador para retornar à página de detalhes **volume / Saúde**.

A nova relação é apresentada na vista de topologia da página de detalhes de volume/Saúde.

Dependendo do SVM de destino especificado durante a configuração ou das opções habilitadas nas configurações avançadas, a relação SnapMirror resultante pode ser uma das várias variações possíveis:

- Se você especificou um SVM de destino que seja executado na mesma ou em uma versão mais recente do ONTAP em comparação com a do volume de origem, uma relação do SnapMirror baseada em replicação de bloco será o resultado padrão.
- Se você especificou um SVM de destino que seja executado na mesma ou em uma versão mais recente do ONTAP em comparação com a do volume de origem, mas ativou a replicação flexível de versão nas configurações avançadas, o resultado será uma relação do SnapMirror com a replicação flexível de versão.
- Se você especificou um SVM de destino que seja executado em uma versão anterior do ONTAP ou uma versão maior do que a do volume de origem e a versão anterior oferecer suporte à replicação flexível de versão, uma relação do SnapMirror com a replicação flexível de versão será o resultado automático.

## Criando uma relação SnapMirror com replicação flexível de versão

Você pode criar uma relação do SnapMirror com a replicação flexível da versão. A replicação flexível da versão permite implementar a proteção do SnapMirror mesmo que os volumes de origem e destino sejam executados em diferentes versões do ONTAP.

## Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.
- As SVMs de origem e destino devem ter uma licença SnapMirror ativada.
- As SVMs de origem e destino devem ser executadas em uma versão do software ONTAP que ofereça suporte à replicação flexível da versão.

O SnapMirror com replicação flexível de versão permite que você implemente a proteção SnapMirror mesmo em ambientes de storage heterogêneos em que nem todo o storage está sendo executado em uma versão do ONTAP. No entanto, as operações espelhadas executadas no SnapMirror com replicação flexível de versão não são executadas tão rapidamente quanto no SnapMirror de replicação de bloco tradicional.

## Passos

1. Exiba a caixa de diálogo **Configurar proteção** para o volume que você deseja proteger.
  - Se estiver a visualizar o separador proteção da página de detalhes de volume / Saúde, clique com o botão direito do rato na vista de topologia que tem o nome de um volume que pretende proteger e selecione **Protect > SnapMirror** no menu.
  - Se você estiver visualizando a exibição Saúde: Todos os volumes, localize um volume que você deseja proteger e clique nele com o botão direito; em seguida, selecione **Protect > SnapMirror** no menu. A caixa de diálogo Configurar proteção é exibida.
2. Clique em **SnapMirror** para visualizar o separador **SnapMirror**.
3. Preencha a área **informações de destino** e a área **Configurações de relacionamento** na caixa de diálogo **Configurar proteção**.

Se você especificar um SVM de destino que seja executado em uma versão anterior do ONTAP do que o volume de origem que você está protegendo e se essa versão anterior suportar replicação flexível de versão, essa tarefa configurará automaticamente o SnapMirror com replicação flexível de versão.

4. Se você especificar um SVM de destino que seja executado na mesma versão do ONTAP do volume de origem, mas ainda desejar configurar o SnapMirror com replicação flexível de versão, clique em **Avançado** para habilitar a replicação flexível de versão e clique em **aplicar**.
5. Clique em **aplicar**.

Regressa à página de detalhes de volume / Saúde.

6. Clique no link do trabalho de configuração de proteção na parte superior da página de detalhes **volume / Saúde**.

As tarefas e os detalhes dos trabalhos são apresentados na página Detalhes do trabalho.

7. Na página de detalhes do **trabalho**, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído.
8. Quando as tarefas de trabalho estiverem concluídas, clique em **voltar** no seu navegador para retornar à página de detalhes **volume / Saúde**.

A nova relação é apresentada na vista de topologia da página de detalhes de volume/Saúde.

## Criando relacionamentos do SnapMirror com replicação flexível com versão com opção de backup

Você pode criar um relacionamento do SnapMirror com a funcionalidade de opção de replicação flexível e backup. A funcionalidade de opção de backup permite que você implemente a proteção SnapMirror e também retenha várias versões de cópias de backup no local de destino.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.
- As SVMs de origem e destino devem ter uma licença SnapMirror ativada.
- As SVMs de origem e destino devem ter uma licença SnapVault ativada.
- As SVMs de origem e destino devem ser executadas em uma versão do software ONTAP que ofereça suporte à replicação flexível da versão.

A configuração do SnapMirror com a funcionalidade de opção de backup permite proteger seus dados com recursos de recuperação de desastres do SnapMirror, como a capacidade de failover de volume, e ao mesmo tempo fornecer recursos de SnapVault, como proteção de várias cópias de backup.

### Passos

1. Exiba a caixa de diálogo **Configurar proteção** para o volume que você deseja proteger.
  - Se estiver a visualizar o separador proteção da página de detalhes de volume / Saúde, clique com o botão direito do rato na topologia para visualizar o nome de um volume que pretende proteger e selecione **Protect > SnapMirror** no menu.
  - Se você estiver visualizando a exibição Saúde: Todos os volumes, localize um volume que você deseja proteger e clique nele com o botão direito; em seguida, selecione **Protect > SnapMirror** no menu. A caixa de diálogo Configurar proteção é exibida.
2. Clique em **SnapMirror** para visualizar o separador **SnapMirror**.
3. Preencha a área **informações de destino** e a área **Configurações de relacionamento** na caixa de diálogo **Configurar proteção**.
4. Clique em **Avançado** para exibir a caixa de diálogo **Configurações avançadas de destino**.
5. Se a caixa de verificação **replicação flexível da versão** ainda não estiver selecionada, selecione-a agora.
6. Marque a caixa de seleção **with backup option** para habilitar o recurso de opção de backup; em seguida, clique em **Apply**.
7. Clique em **aplicar**.

Regressa à página de detalhes de volume / Saúde.

8. Clique no link do trabalho de configuração de proteção na parte superior da página de detalhes **volume / Saúde**.

As tarefas e os detalhes dos trabalhos são apresentados na página Detalhes do trabalho.

9. Na página de detalhes do **trabalho**, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído.

10. Quando as tarefas de trabalho estiverem concluídas, clique em **voltar** no seu navegador para retornar à página de detalhes **volume / Saúde**.

A nova relação é apresentada na vista de topologia da página de detalhes de volume/Saúde.

## Configurar as definições de eficiência do destino

Você pode configurar configurações de eficiência de destino, como deduplicação, compactação, crescimento automático e garantia de espaço em um destino de proteção usando a caixa de diálogo Configurações avançadas de destino. Use essas configurações quando quiser maximizar a utilização de espaço em um destino ou volume secundário.

### Antes de começar

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

Por padrão, as configurações de eficiência correspondem às do volume de origem, exceto as configurações de compactação em uma relação SnapVault, que são desativadas por padrão.

### Passos

1. Clique na guia **SnapMirror** ou na guia **SnapVault** na caixa de diálogo **Configurar proteção**, dependendo do tipo de relacionamento que você está configurando.
2. Clique em **Avançado** na área **informações de destino**.

A caixa de diálogo Configurações avançadas de destino é aberta.

3. Ative ou desative as configurações de eficiência para deduplicação, compactação, crescimento automático e garantia de espaço, conforme necessário.
4. Clique em **Apply** para salvar suas seleções e retornar à caixa de diálogo **Configurar proteção**.

## Criando agendas SnapMirror e SnapVault

Você pode criar agendas básicas ou avançadas de SnapMirror e SnapVault para permitir transferências automáticas de proteção de dados em uma fonte ou volume primário para que as transferências ocorram com mais frequência ou com menos frequência, dependendo da frequência com que os dados mudam em seus volumes.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você já deve ter concluído a área informações de destino na caixa de diálogo Configurar proteção.
- Você deve ter configurado o Workflow Automation para executar esta tarefa.

### Passos

1. Na guia **SnapMirror** ou na guia **SnapVault** da caixa de diálogo **Configurar proteção**, clique no link **criar agendamento** na área **Configurações de relacionamento**.

A caixa de diálogo criar agendamento é exibida.

2. No campo **Nome da programação**, digite o nome que deseja dar à programação.

3. Selecione uma das seguintes opções:

◦ **Básico**

Selecione se pretende criar uma agenda de estilo de intervalo básico.

◦ **Avançado**

Selecione se você deseja criar um cronograma de estilo cron.

4. Clique em **criar**.

A nova programação é apresentada na lista pendente Agenda SnapMirror ou Programação SnapVault.

## **Criando relações em cascata ou fanout para estender a proteção de uma relação de proteção existente**

Você pode estender a proteção de um relacionamento existente criando um fanout do volume de origem ou uma cascata do volume de destino de um relacionamento existente. Você pode fazer isso quando precisar copiar dados de um site para muitos sites ou fornecer proteção adicional criando mais backups.

Você pode estender a proteção a volumes usando o grupo consistência, que é um contêiner que contém vários volumes para que você possa gerenciar todos os volumes como uma entidade. Você pode exibir o grupo de consistência de sincronização ativa do SnapMirror e a relação de grupo de consistência síncrona na página relacionamentos do Gerenciador Unificado.

### **Antes de começar**

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

### **Passos**

1. Clique em **proteção > relacionamentos**. Como alternativa, você visualiza as relações na página Detalhes do volume.
2. Na página **relacionamentos de volume**, selecione a relação SnapMirror a partir da qual deseja estender a proteção.
3. Na barra de ação, clique em **Extend Protection**.
4. No menu, selecione **de origem** ou **de destino**, dependendo se você está criando uma relação de fanout da fonte ou uma relação em cascata do destino.
5. Selecione **com SnapMirror** ou **com SnapVault** dependendo do tipo de relação de proteção que você está criando.

A caixa de diálogo **Configurar proteção** é exibida.



Isto pode ser conseguido a partir da página de detalhes de relação unificada/relação de volume e volume/Saúde.

6. Preencha as informações conforme indicado na caixa de diálogo **Configurar proteção**.

## Editar relações de proteção a partir da página relacionamentos de volume

Você pode editar relacionamentos de proteção existentes para alterar a taxa de transferência máxima, a política de proteção ou o cronograma de proteção. Você pode editar um relacionamento para diminuir a largura de banda usada para transferências ou aumentar a frequência de transferências agendadas porque os dados estão mudando com frequência.

### Antes de começar

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

Os volumes selecionados devem ser destinos de relação de proteção. Não é possível editar relacionamentos quando os volumes de origem, volumes de compartilhamento de carga ou volumes que não são o destino de uma relação SnapMirror ou SnapVault estão selecionados.

### Passos

1. Na página **relacionamentos de volume**, selecione na lista volumes um ou mais volumes no mesmo SVM para o qual você deseja editar as configurações de relacionamento e selecione **Editar** na barra de ferramentas.

A caixa de diálogo Editar relacionamento é exibida.

2. Na caixa de diálogo **Editar relacionamento**, edite a taxa máxima de transferência, a política de proteção ou o cronograma de proteção, conforme necessário.
3. Clique em **aplicar**.

As alterações são aplicadas às relações selecionadas.

## Editar relações de proteção a partir da página de detalhes de volume / Saúde

Você pode editar relacionamentos de proteção existentes para alterar a taxa de transferência máxima atual, a política de proteção ou o cronograma de proteção. Você pode editar um relacionamento para diminuir a largura de banda usada para transferências ou aumentar a frequência de transferências agendadas porque os dados estão mudando com frequência.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter instalado e configurado o Workflow Automation.

Os volumes selecionados devem ser destinos de relação de proteção. Não é possível editar relacionamentos quando os volumes de origem, volumes de compartilhamento de carga ou volumes que não são o destino de uma relação SnapMirror ou SnapVault estão selecionados.

### Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, localize na topologia a relação de proteção que deseja editar e clique com o botão direito do Mouse nela.
2. Selecione **Editar** no menu.

Alternativamente, no menu **ações**, selecione **relacionamento** > **Editar** para editar a relação para a qual



você está visualizando os detalhes no momento.

A caixa de diálogo **Editar relacionamento** é exibida.

3. Na caixa de diálogo Editar relacionamento, edite a taxa máxima de transferência, a política de proteção ou o cronograma de proteção, conforme necessário.
4. Clique em **aplicar**.

As alterações são aplicadas às relações selecionadas.

## Criando uma política de SnapMirror para maximizar a eficiência de transferência

Você pode criar uma política SnapMirror para especificar a prioridade de transferência SnapMirror para relacionamentos de proteção. As políticas do SnapMirror permitem maximizar a eficiência de transferência da origem para o destino, atribuindo prioridades para que as transferências de prioridade mais baixa sejam agendadas para serem executadas após as transferências de prioridade normal.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.
- Esta tarefa pressupõe que você já concluiu a área informações de destino na caixa de diálogo Configurar proteção.

### Passos

1. Na guia **SnapMirror** da caixa de diálogo **Configurar proteção**, clique no link **criar política** na área **Configurações de relacionamento**.

A caixa de diálogo criar política de SnapMirror é exibida.

2. No campo **Policy Name** (Nome da política), digite um nome que você deseja atribuir à política.
3. No campo **prioridade de transferência**, selecione a prioridade de transferência que deseja atribuir à política.
4. No campo **comentário**, insira um comentário opcional para a política.
5. Clique em **criar**.

A nova política é exibida na lista suspensa Política de SnapMirror.

## Criando uma política de SnapVault para maximizar a eficiência de transferência

Você pode criar uma nova política de SnapVault para definir a prioridade para uma transferência de SnapVault. Você usa políticas para maximizar a eficiência das transferências do primário para o secundário em um relacionamento de proteção.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

- Você já deve ter concluído a área informações de destino na caixa de diálogo Configurar proteção.

### Passos

1. Na guia **SnapVault** da caixa de diálogo **Configurar proteção**, clique no link **criar política** na área **Configurações de relacionamento**.

É apresentado o separador SnapVault.

2. No campo **Policy Name** (Nome da política), digite o nome que deseja atribuir à política.
3. No campo **prioridade de transferência**, selecione a prioridade de transferência que deseja atribuir à política.
4. **Opcional:** no campo **comentário**, insira um comentário para a política.
5. Na área **Etiqueta de replicação**, adicione ou edite um rótulo de replicação, conforme necessário.
6. Clique em **criar**.

A nova política é exibida na lista suspensa criar política.

## Abortar uma transferência ativa de proteção de dados a partir da página relacionamentos de volume

Você pode cancelar uma transferência de proteção de dados ativa quando quiser interromper uma replicação do SnapMirror em andamento. Você também pode limpar o ponto de verificação reiniciar para transferências subsequentes à transferência da linha de base. Você pode cancelar uma transferência quando ela entrar em conflito com outra operação, como uma movimentação de volume.



Não é possível abortar relacionamentos de volumes protegidos pelo Grupo de consistência.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

A ação de cancelamento não é exibida nas seguintes instâncias:

- Se as configurações RBAC não permitirem essa ação: Por exemplo, se você tiver apenas Privileges de operador
- Quando o ID do volume é desconhecido: Por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

Não é possível limpar o ponto de verificação reiniciar para uma transferência de linha de base.

### Passos

1. Para cancelar transferências para um ou mais relacionamentos de proteção, na página **relacionamentos de volume**, selecione um ou mais volumes e, na barra de ferramentas, clique em **Cancelar**.

A caixa de diálogo Cancelar transferência é exibida.

2. Se quiser limpar o ponto de verificação reiniciar para uma transferência que não seja uma transferência de linha de base, selecione **Limpar pontos de verificação**.

### 3. Clique em **continuar**.

A caixa de diálogo Cancelar transferência é fechada e o status da tarefa de abortar é exibido na parte superior da página relacionamentos de volume, juntamente com um link para os detalhes da tarefa.

### 4. **Opcional:** clique no link **Exibir detalhes** para ir para a página de detalhes **trabalho** para obter detalhes adicionais e para ver o progresso do trabalho.

## Abortar uma transferência ativa de proteção de dados a partir da página de detalhes de volume / Saúde

Você pode cancelar uma transferência de proteção de dados ativa quando quiser interromper uma replicação do SnapMirror em andamento. Você também pode limpar o ponto de verificação reiniciar para uma transferência se não for uma transferência de linha de base. Você pode cancelar uma transferência quando ela entrar em conflito com outra operação, como uma movimentação de volume.



Não é possível abortar relacionamentos de volumes protegidos pelo Grupo de consistência.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

A ação de cancelamento não é exibida nas seguintes instâncias:

- Se as configurações RBAC não permitirem essa ação: Por exemplo, se você tiver apenas Privileges de operador
- Quando o ID do volume é desconhecido: Por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

Não é possível limpar o ponto de verificação reiniciar para uma transferência de linha de base.

### Passos

#### 1. Na guia **proteção** da página de detalhes **volume / Saúde**, clique com o botão direito do Mouse na relação na exibição de topologia para a transferência de dados que deseja abortar e selecione **Cancelar**.

A caixa de diálogo Cancelar transferência é exibida.

#### 2. Se quiser limpar o ponto de verificação reiniciar para uma transferência que não seja uma transferência de linha de base, selecione **Limpar pontos de verificação**.

#### 3. Clique em **continuar**.

A caixa de diálogo Cancelar transferência é fechada e o status da operação de cancelamento é exibido na parte superior da página de detalhes de volume / Saúde, juntamente com um link para os detalhes do trabalho.

#### 4. **Opcional:** clique no link **Exibir detalhes** para ir para a página de detalhes **trabalho** para obter detalhes adicionais e para ver o progresso do trabalho.

#### 5. Clique em cada tarefa de trabalho para ver os seus detalhes.

#### 6. Clique na seta para trás do seu navegador para retornar à página de detalhes **volume / Saúde**.

A operação de cancelamento é concluída quando todas as tarefas de trabalho forem concluídas com êxito.

## Mantendo uma relação de proteção a partir da página relacionamentos de volume

Na página relacionamentos de volume, você pode silenciar uma relação de proteção para impedir temporariamente a ocorrência de transferências de dados. Você pode desativar um relacionamento quando quiser criar uma cópia Snapshot de um volume de destino do SnapMirror que contém um banco de dados e deseja garantir que seu conteúdo esteja estável durante a operação de cópia Instantânea.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

A ação quiesce não é exibida nos seguintes casos:

- Se as configurações RBAC não permitirem essa ação; por exemplo, se você tiver apenas Privileges de operador
- Quando o ID do volume é desconhecido; por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto
- Quando você não emparelhou o Workflow Automation e o Unified Manager

### Passos

1. Para obter transferências para um ou mais relacionamentos de proteção, na página **relacionamentos de volume**, selecione um ou mais volumes e, na barra de ferramentas, clique em **quiesce**.

A caixa de diálogo quiesce é exibida.

2. Clique em **continuar**.

O status do trabalho quiesce é exibido na parte superior da página de detalhes de volume / Saúde, juntamente com um link para os detalhes do trabalho.

3. Clique no link **Exibir detalhes** para ir para a página de detalhes **trabalho** para obter detalhes adicionais e progresso do trabalho.
4. **Opcional:** clique na seta **voltar** no seu navegador para retornar à página **relacionamentos por volume**.

O trabalho quiesce é concluído quando todas as tarefas de trabalho são concluídas com êxito.

## Mantendo uma relação de proteção a partir da página de detalhes de volume / Saúde

Você pode silenciar uma relação de proteção para impedir temporariamente a ocorrência de transferências de dados. Você pode desativar um relacionamento quando quiser criar uma cópia Snapshot de um volume de destino do SnapMirror que contém um banco de dados e deseja garantir que seu conteúdo esteja estável durante a cópia Snapshot.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

A ação quiesce não é exibida nos seguintes casos:

- Se as configurações RBAC não permitirem essa ação, por exemplo, se você tiver apenas Privileges de operador
- Quando o ID do volume é desconhecido, por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto
- Quando você não emparelhou o Workflow Automation e o Unified Manager

### Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, clique com o botão direito do Mouse na relação na exibição de topologia para a relação de proteção que você deseja silenciar.
2. Selecione **quiesce** no menu.
3. Clique em **Yes** para continuar.

O status do trabalho quiesce é exibido na parte superior da página de detalhes de volume / Saúde, juntamente com um link para os detalhes do trabalho.

4. Clique no link **Exibir detalhes** para ir para a página de detalhes **trabalho** para obter detalhes adicionais e progresso do trabalho.
5. **Opcional:** clique na seta para trás do seu navegador para retornar à página de detalhes **volume / Saúde**.

O trabalho quiesce é concluído quando todas as tarefas de trabalho são concluídas com êxito.

## Quebrar uma relação de SnapMirror a partir da página relacionamentos de volume

É possível interromper uma relação de proteção para interromper as transferências de dados entre um volume de origem e um volume de destino em uma relação do SnapMirror. Você pode interromper um relacionamento quando quiser migrar dados, para recuperação de desastres ou para teste de aplicações. O volume de destino é alterado para um volume de leitura/gravação. Você não pode quebrar um relacionamento SnapVault.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.


### Passos

1. Na página **relacionamentos de volume**, selecione um ou mais volumes com relacionamentos de proteção para os quais você deseja interromper as transferências de dados e, na barra de ferramentas, clique em **quebrar**.

É apresentada a caixa de diálogo Break Relationship (interromper relação).

2. Clique em **continuar** para quebrar o relacionamento.
3. Na página **relacionamentos de volume**, verifique na coluna **Estado do relacionamento** se o

relacionamento está quebrado.

A coluna Estado do relacionamento está oculta por padrão, portanto, talvez seja necessário selecioná-la na lista Mostrar/ocultar coluna .

## Removendo uma relação de proteção da página relacionamentos de volume

Na página relacionamentos de volume, você pode remover uma relação de proteção para excluir permanentemente uma relação existente entre a origem e o destino selecionados: Por exemplo, quando você deseja criar uma relação usando um destino diferente. Esta operação remove todos os metadados e não pode ser desfeita.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

### Passos

1. Na página **relacionamentos de volume**, selecione um ou mais volumes com relacionamentos de proteção que deseja remover e, na barra de ferramentas, clique em **Remover**.

A caixa de diálogo Remover relacionamento é exibida.

2. Clique em **continuar** para remover o relacionamento.

A relação é removida da página relacionamentos de volume.

## Retomar as transferências agendadas em um relacionamento quiesced da página relacionamentos do volume

Depois de ter concluído um relacionamento para impedir que as transferências agendadas ocorram, você pode usar **Resume** para reativar as transferências agendadas para que os dados no volume de origem ou principal estejam protegidos. As transferências são retomadas a partir de um ponto de verificação, se houver, no próximo intervalo de transferência programado.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

Você não pode selecionar mais de 10 relacionamentos quiesced nos quais retomar as transferências.

### Passos

1. Na página volume **relacionamentos**, selecione um ou mais volumes com relacionamentos quiesced e, na barra de ferramentas, clique em **Resume**.
2. Na caixa de diálogo **Resume**, clique em **Continue**.

Você será retornado à página relacionamentos de volume.

3. Para visualizar as tarefas relacionadas e acompanhar o seu progresso, clique no link da tarefa que é

exibido na parte superior da página **relacionamentos de volume**.

4. Execute um dos seguintes procedimentos:

- Se for apresentado apenas um trabalho, na página Detalhes do trabalho, clique em **Atualizar** para atualizar a lista tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído.
- Se for apresentado mais de um trabalho,
  - i. Na página trabalhos, clique no trabalho para o qual deseja exibir os detalhes.
  - ii. Na página Detalhes do trabalho, clique em **Atualizar** para atualizar a lista tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído. Após o término dos trabalhos, as transferências de dados são retomadas no próximo intervalo de transferência programado.

## **Retomar as transferências agendadas numa relação quiesced a partir da página de detalhes de volume / Saúde**

Depois de ter silenciado um relacionamento para impedir que as transferências agendadas ocorram, você pode usar **Resume** na página de detalhes de volume / Saúde para reativar as transferências agendadas para que os dados na origem ou no volume primário sejam protegidos. As transferências são retomadas a partir de um ponto de verificação, se houver, no próximo intervalo de transferência programado.

### **Antes de começar**

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

### **Passos**

1. Na guia **proteção** da página de detalhes **volume / Saúde**, clique com o botão direito do Mouse na exibição de topologia uma relação quiesced que você deseja retomar.

Em alternativa, selecione **Resume** no menu **ações > relacionamento**.

2. Na caixa de diálogo **Resume**, clique em **Continue**.

Regressa à página de detalhes de volume / Saúde.

3. Para visualizar as tarefas relacionadas e acompanhar o seu progresso, clique no link do trabalho que é exibido na parte superior da página de detalhes **volume / Saúde**.
4. Na página de detalhes do **trabalho**, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho está concluído.

Após a conclusão dos trabalhos, as transferências de dados são retomadas no próximo intervalo de transferência programado.

## **Inicializando ou atualizando relacionamentos de proteção a partir da página relacionamentos de volume**

Na página relacionamentos de volume, você pode executar uma transferência de linha

de base pela primeira vez em um novo relacionamento de proteção ou atualizar um relacionamento se ele já estiver inicializado e você quiser executar uma atualização incremental manual e não programada para transferir imediatamente.



Não é possível inicializar ou atualizar volumes protegidos por grupos de consistência.

#### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Tem de ter configurado o OnCommand Workflow Automation.

#### Passos

1. Na página **relacionamentos de volume**, clique com o botão direito do Mouse em um volume e selecione um ou mais volumes com relacionamentos que você deseja atualizar ou inicializar e, na barra de ferramentas, clique em **Inicializar/Atualizar**.

A caixa de diálogo **Inicializar/Atualizar** é exibida.

2. Na guia **Opções de transferência**, selecione uma prioridade de transferência e a taxa de transferência máxima.
3. Clique em **cópias snapshot de origem**; em seguida, na coluna **cópia Snapshot**, clique em **predefinição**.

A caixa de diálogo Selecionar cópia Snapshot de origem é exibida.

4. Se você quiser especificar uma cópia Snapshot existente em vez de transferir a cópia Snapshot padrão, clique em **cópia Snapshot existente** e selecione uma cópia Snapshot na lista.
5. Clique em **Enviar**.

Você será retornado à caixa de diálogo **Inicializar/Atualizar**.

6. Se você selecionou mais de uma fonte para inicializar ou atualizar, clique em **Default** para a próxima fonte para a qual deseja especificar uma cópia Snapshot existente.
7. Clique em **Enviar** para iniciar o trabalho de inicialização ou atualização.

O trabalho de inicialização ou atualização é iniciado, você retorna à página relacionamentos de volume e um link trabalhos é exibido na parte superior da página.

8. **Opcional:** clique em **Exibir trabalhos** na exibição **Saúde: Todos os volumes** para rastrear o status de cada tarefa de inicialização ou atualização.

É apresentada uma lista filtrada de trabalhos.

9. **Opcional:** clique em cada trabalho para ver seus detalhes.
10. **Opcional:** clique na seta **voltar** no seu navegador para retornar à página **relacionamentos por volume**.

A operação de inicialização ou atualização é concluída quando todas as tarefas são concluídas com êxito.

## Inicializando ou atualizando relacionamentos de proteção a partir da página de detalhes de volume / Saúde

Você pode executar uma transferência de linha de base pela primeira vez em um novo



relacionamento de proteção ou atualizar um relacionamento se ele já estiver inicializado e desejar executar uma atualização incremental manual e não programada para transferir dados imediatamente.

**NOTA:** Não é possível inicializar ou atualizar volumes protegidos por grupos de consistência.

#### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Tem de ter configurado o OnCommand Workflow Automation.

#### Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, localize na topologia a relação de proteção que você deseja inicializar ou atualizar e clique com o botão direito do Mouse nela.

2. Selecione **Inicializar/Atualizar** no menu.

Alternativamente, no menu **ações**, selecione **relacionamento > Inicializar/Atualizar** para inicializar ou atualizar a relação para a qual você está visualizando os detalhes no momento.

A caixa de diálogo Inicializar/Atualizar é exibida.

3. Na guia **Opções de transferência**, selecione uma prioridade de transferência e a taxa de transferência máxima.

4. Clique em **cópias snapshot de origem**; em seguida, na coluna **cópia Snapshot**, clique em **predefinição**.

A caixa de diálogo Selecionar cópia Snapshot de origem é exibida.

5. Se você quiser especificar uma cópia Snapshot existente em vez de transferir a cópia Snapshot padrão, clique em **cópia Snapshot existente** e selecione uma cópia Snapshot na lista.

6. Clique em **Enviar**.

Você será retornado à caixa de diálogo Inicializar/Atualizar.

7. Se você selecionou mais de uma fonte para inicializar ou atualizar, clique em **Default** para a próxima fonte de leitura/gravação para a qual deseja especificar uma cópia Snapshot existente.

Não é possível selecionar uma cópia Snapshot diferente para volumes de proteção de dados.

8. Clique em **Enviar** para iniciar o trabalho de inicialização ou atualização.

O trabalho de inicialização ou atualização é iniciado, você retorna à página de detalhes de volume / Saúde e um link trabalhos é exibido na parte superior da página.

9. **Opcional:** clique em **Exibir trabalhos** na página de detalhes **volume / Saúde** para rastrear o status de cada tarefa de inicialização ou atualização.

É apresentada uma lista filtrada de trabalhos.

10. **Opcional:** clique em cada trabalho para ver seus detalhes.

11. **Opcional:** clique na seta para trás do seu navegador para retornar à página de detalhes **volume / Saúde**.

A operação de inicialização ou atualização é concluída quando todas as tarefas de trabalho forem concluídas com êxito.

## Ressincronizar relacionamentos de proteção a partir da página relacionamentos de volume

Na página relacionamentos de volume, você pode ressincronizar um relacionamento para recuperar de um evento que desabilitou o volume de origem ou quando deseja alterar a fonte atual para um volume diferente.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

### Passos

1. Na página **relacionamentos de volume**, selecione um ou mais volumes com relacionamentos quiesced e, na barra de ferramentas, clique em **Resynchronize**.

A caixa de diálogo Resyncronizar é exibida.

2. Na guia **Opções de ressincronização**, selecione uma prioridade de transferência e a taxa de transferência máxima.
3. Clique em **cópias snapshot de origem**; em seguida, na coluna **cópia Snapshot**, clique em **predefinição**.

A caixa de diálogo Selecionar cópia Snapshot de origem é exibida.

4. Se você quiser especificar uma cópia Snapshot existente em vez de transferir a cópia Snapshot padrão, clique em **cópia Snapshot existente** e selecione uma cópia Snapshot na lista.
5. Clique em **Enviar**.

Você será retornado à caixa de diálogo Resyncronizar.

6. Se você selecionou mais de uma fonte para ressincronizar, clique em **Default** para a próxima fonte para a qual deseja especificar uma cópia Snapshot existente.
7. Clique em **Enviar** para iniciar o trabalho de ressincronização.

O trabalho de ressincronização é iniciado, você retorna à página relacionamentos de volume e um link trabalhos é exibido na parte superior da página.

8. **Opcional:** clique em **Exibir trabalhos** na página **relacionamentos de volume** para rastrear o status de cada trabalho de ressincronização.

É apresentada uma lista filtrada de trabalhos.

9. **Opcional:** clique na seta **voltar** no seu navegador para retornar à página **relacionamentos por volume**.

A operação de ressincronização é concluída quando todas as tarefas de trabalho forem concluídas com êxito.

## Reverter relações de proteção a partir da página relacionamentos de volume

Quando um desastre desativa o volume de origem em sua relação de proteção, você pode usar o volume de destino para servir dados convertendo-os em um volume de leitura/gravação enquanto você reparar ou substituir a origem. Quando a origem estiver

novamente disponível para receber dados, você poderá usar a operação de resincronização reversa para estabelecer a relação na direção inversa, sincronizando os dados na origem com os dados no destino de leitura/gravação.

#### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.
- O relacionamento não deve ser um relacionamento SnapVault.
- Uma relação de proteção já deve existir.
- A relação de proteção deve ser quebrada.
- Tanto a origem como o destino devem estar online.
- A origem não deve ser o destino de outro volume de proteção de dados.
- Quando você executa essa tarefa, os dados na fonte mais recente do que os dados na cópia Snapshot comum são excluídos.
- Políticas e programações criadas em relacionamentos de resincronização reversa são as mesmas que as da relação de proteção original.

Se as políticas e agendas não existirem, elas são criadas.

#### Passos

1. Na página **relacionamentos de volume**, selecione um ou mais volumes com relacionamentos que você deseja reverter e, na barra de ferramentas, clique em **Reverse Resync**.

A caixa de diálogo Reverse Resync (Reverse Resync) é exibida.

2. Verifique se as relações exibidas na caixa de diálogo **Reverse Resync** são aquelas para as quais você deseja executar a operação de resincronização reversa e clique em **Submit**.

A operação de resincronização reversa é iniciada, você retorna à página relacionamentos de volume e um link trabalhos é exibido na parte superior da página.

3. **Opcional:** clique em **Exibir trabalhos** na página **relacionamentos de volume** para rastrear o status de cada tarefa de resincronização reversa.

É apresentada uma lista filtrada de trabalhos relacionados com esta operação.

4. **Opcional:** clique na seta **voltar** no seu navegador para retornar à página **relacionamentos por volume**.

A operação de resincronização reversa é concluída quando todas as tarefas de trabalho forem concluídas com êxito.

## Restaurar dados utilizando as páginas de detalhes de volume e volume / Saúde

Você pode restaurar arquivos, diretórios ou um volume inteiro sobrescritos ou excluídos de uma cópia Snapshot usando o recurso de restauração nas páginas de detalhes de volume e volume / integridade.

#### Antes de começar

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



Observe os seguintes pontos:

- Não é possível restaurar fluxos de ficheiros NTFS.
- A opção de restauração não está disponível quando:
  - O ID do volume é desconhecido: Por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto.
  - O volume é configurado para replicação síncrona do SnapMirror.

## Passos

1. No painel de navegação esquerdo, vá para **Storage > volumes**.
2. Selecione o volume e clique no botão **Restore**. Em alternativa, clique no volume para ir para **volume / Detalhes do estado > ações > Restaurar**. A caixa de diálogo Restaurar é exibida. Para obter informações sobre esta página, "[Caixa de diálogo Restaurar](#)" consulte .
3. Selecione o volume e a cópia Snapshot a partir da qual você deseja restaurar dados, se diferente do padrão.
4. Selecione os itens que deseja restaurar, por exemplo, o LUN de origem.

Você pode restaurar todo o volume ou especificar pastas e arquivos que deseja restaurar.

5. Selecione o local para o qual deseja restaurar os itens selecionados: **Localização original** ou **localização existente alternativa**.
6. Se você selecionar um local alternativo existente, execute um dos seguintes procedimentos:
  - No campo de texto Restaurar caminho, digite o caminho do local para o qual deseja restaurar os dados e clique em **Selecionar diretório**.
  - Clique em **Procurar** para iniciar a caixa de diálogo Procurar diretórios e concluir as seguintes etapas:
    - i. Selecione o cluster de destino, a VM de storage (SVM) e o volume para o qual você deseja restaurar.
    - ii. Na tabela Nome, selecione um nome de diretório que tem de ser restaurado.
    - iii. Clique em **Select Directory**.
7. Clique em **Restaurar**.

O processo de restauração é iniciado. Um trabalho é criado no back-end para concluir o processo de restauração.

8. Se pretender ver o progresso do trabalho, a partir do painel de navegação esquerdo, navegue até **proteção > tarefas** para ver o estado do trabalho de restauro a partir da lista de trabalhos.



Se uma operação de restauração falhar entre clusters de HA do Cloud Volumes ONTAP com um erro NDMP, talvez seja necessário adicionar uma rota explícita da AWS no cluster de destino para que o destino possa se comunicar com o LIF de gerenciamento de cluster do sistema de origem. Execute esta etapa de configuração usando o BlueXP .

## Quais são os pools de recursos

Os pools de recursos são grupos de agregados criados por um administrador de storage usando o Unified Manager para fornecer provisionamento a aplicações de parceiros para gerenciamento de backup.

Você pode agrupar seus recursos com base em atributos como desempenho, custo, localização física ou disponibilidade. Agrupando recursos relacionados em um pool, você pode tratar o pool como uma única unidade para monitoramento e provisionamento. Isso simplifica o gerenciamento desses recursos e permite um uso mais flexível e eficiente do storage.

Durante o provisionamento de storage secundário, o Unified Manager determina o agregado mais adequado no pool de recursos para proteção usando os seguintes critérios:

- O agregado é um agregado de dados (não um agregado de raiz) e está ON-LINE.
- O agregado está em um nó de cluster de destino cuja versão do ONTAP seja igual ou maior que a versão principal do cluster de origem.
- O agregado tem o maior espaço disponível de todos os agregados no pool de recursos.
- Após o provisionamento do volume de destino, o espaço agregado está dentro do limite quase cheio e quase sobrecarregado definido para o agregado (limite global ou local, o que for aplicável).
- O número de volumes FlexVol no nó de destino não deve exceder o limite da plataforma.

## Criando pools de recursos

Você pode usar a caixa de diálogo criar pool de recursos para agrupar agregados para fins de provisionamento.

### Antes de começar

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

### Passos

Os pools de recursos podem conter agregados de clusters diferentes, mas o mesmo agregado não pode pertencer a pools de recursos diferentes.

1. No painel de navegação esquerdo, clique em **proteção > pools de recursos**.
2. Na página **pools de recursos**, clique em **criar**.
3. Siga as instruções na caixa de diálogo **criar pool de recursos** para fornecer um nome e uma descrição e adicionar agregados como membros ao pool de recursos que você deseja criar.

## Editando pools de recursos

Você pode editar um pool de recursos existente quando quiser alterar o nome do pool de recursos e a descrição.

### Antes de começar

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

O botão **Editar** é ativado somente quando um pool de recursos é selecionado. Se for selecionado mais de um pool de recursos, o botão **Editar** será desativado.

## Passos

1. No painel de navegação esquerdo, clique em **proteção > pools de recursos**.
2. Selecione um pool de recursos na lista.
3. Clique em **Editar**.

A janela Editar pool de recursos é exibida.

4. Edite o nome e a descrição do pool de recursos conforme necessário.
5. Clique em **Salvar**.

O novo nome e descrição são exibidos na lista de pool de recursos.

## Exibindo inventário de pools de recursos

Você pode usar a página pools de recursos para exibir o inventário do pool de recursos e monitorar a capacidade restante de cada pool de recursos.

### Antes de começar

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

### Passo

1. No painel de navegação esquerdo, clique em **proteção > pools de recursos**.

O inventário do pool de recursos é exibido.

## Adicionando membros do pool de recursos

Um pool de recursos consiste em vários agregados de membros. Você pode adicionar agregados a pools de recursos existentes para aumentar a quantidade de espaço disponível para o provisionamento de volume secundário.

### Antes de começar

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

Você não pode adicionar mais de 200 agregados a um pool de recursos de uma só vez. Os agregados mostrados na caixa de diálogo agregados não pertencem a nenhum outro pool de recursos.

### Passos

1. No painel de navegação esquerdo, clique em **proteção > pools de recursos**.
2. Selecione um pool de recursos na lista **pools de recursos**.

Os membros do pool de recursos são exibidos na área abaixo da lista de pool de recursos.

3. Na área de membro do pool de recursos, clique em **Add**.

A caixa de diálogo agregados é exibida.

4. Selecione um ou mais agregados.
5. Clique em **Add**.

A caixa de diálogo é fechada e os agregados são exibidos na lista de membros do pool de recursos selecionado.

## Remoção de agregados de pools de recursos

Você pode remover agregados de um pool de recursos existente: Por exemplo, quando você deseja usar um agregado para algum outro propósito.

### Antes de começar

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

Os membros do pool de recursos são exibidos somente quando um pool de recursos é selecionado.

### Passos

1. No painel de navegação esquerdo, clique em **proteção > pools de recursos**.
2. Selecione o pool de recursos do qual você deseja remover agregados de membros.

A lista de agregados de membros é exibida no painel Membros.

3. Selecione um ou mais agregados.

O botão **Remove** está ativado.

4. Clique em **Remover**.

É apresentada uma caixa de diálogo de aviso.

5. Clique em **Yes** para continuar.

Os agregados selecionados são removidos do painel Membros.

## Excluindo pools de recursos

Você pode excluir pools de recursos quando eles não forem mais necessários. Por exemplo, você pode querer redistribuir os agregados de membros de um pool de recursos para vários outros pools de recursos, tornando o pool de recursos original obsoleto.

### Antes de começar

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

O botão **Delete** é ativado somente quando pelo menos um pool de recursos estiver selecionado.

### Passos

1. No painel de navegação esquerdo, clique em **proteção > pools de recursos**.
2. Selecione o pool de recursos que deseja excluir.
3. Clique em **Excluir**.

O pool de recursos é removido da lista de pool de recursos e seus agregados são removidos da lista de membros.

## Monitoramento de relacionamentos de proteção de recuperação de desastres da VM Storage

O Active IQ Unified Manager é compatível com o monitoramento de relacionamentos de recuperação de desastres de VM de storage, que oferece recuperação de desastres na granularidade de um nível de VM de storage. A recuperação de desastres da VM de armazenamento permite a recuperação de dados presentes nos volumes constituintes da VM de armazenamento e a recuperação da configuração da VM de armazenamento.

Uma relação de recuperação de desastres de VM de storage é criada da VM de storage de origem para a VM de storage de destino, a fim de fornecer recuperação assíncrona de desastres. Você pode selecionar para replicar toda ou um subconjunto da configuração da VM de armazenamento (excluindo a configuração de rede e protocolo) juntamente com os volumes de dados baseados na configuração do cluster.

Após a configuração do relacionamento de recuperação de desastres da VM de armazenamento, quando a VM de armazenamento de origem fica indisponível devido a falha de hardware ou desastre ambiental, a VM de armazenamento de destino é iniciada, o que fornece acesso aos dados com o mínimo de interrupção. Da mesma forma, quando a VM de armazenamento de origem fica disponível, ela é ressincronizada com a VM de armazenamento de destino e, em seguida, a fonte reinicia para fornecer dados. Você pode usar os comandos SnapMirror para configurar e gerenciar o relacionamento de recuperação de desastres da VM de storage.

### Monitoramento de VMs de armazenamento usando a página relacionamentos

Você pode monitorar as relações de recuperação de desastres da VM de storage na página relacionamentos na SEÇÃO PROTEÇÃO do INVENTÁRIO. Por padrão, a página relacionamentos lista apenas as relações de nível superior à medida que o filtro relações constituintes é aplicado.

#### Antes de começar

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

Você usa filtros para exibir os relacionamentos de recuperação de desastres da VM de storage.

#### Passos

1. No painel de navegação esquerdo, clique em **PROTECTION > relationships**.

A página exibe todos os tipos de relacionamentos: Volume, grupo de consistência e relações de VM de armazenamento.

2. Clique em **Filter** e selecione **Relationship Object Type** e **Storage VM** para visualizar apenas as relações de recuperação de desastres da VM de armazenamento.
3. Clique em **Apply Filter** (aplicar filtro).



Você deve limpar o filtro relacionamentos constituintes para visualizar todas as relações de proteção.

A página exibe somente relacionamentos de recuperação de desastres da VM de storage.



## Exibindo relacionamentos de proteção da página Storage VMs

Usando a página Storage VMs, você pode visualizar o status das relações de recuperação de desastres das VMs de storage existentes.

### Antes de começar

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

Você também pode examinar detalhes dos relacionamentos de proteção, incluindo status de transferência e atraso, detalhes de origem e destino. Você pode agendar relatórios ou fazer download de relatórios existentes no formato desejado. O botão **Mostrar/Ocultar** permite que você adicione as colunas necessárias aos relatórios, pois elas não são exibidas por padrão.

### Passos

1. No painel de navegação esquerdo, clique em **STORAGE > Storage VMs**.
2. No menu **VIEW**, selecione **Relationship > All relationships**.

A visualização relacionamento: Todas as relações é exibida com todas as VMs de armazenamento configuradas.

## Visualização de VMs de armazenamento com base no status de proteção

Você pode usar a página Storage VMs do Inventário para visualizar todas as VMs de storage no Active IQ Unified Manager e filtrar as VMs de storage com base em seu status de proteção.

### Antes de começar

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

Uma nova função de proteção de coluna é adicionada à visualização de VMs de storage que fornece informações sobre se a VM de storage está protegida ou não protegida.



Se um cluster de origem não for adicionado ao Active IQ Unified Manager, todas as informações relacionadas a esse cluster não estarão disponíveis nas grades.

### Passos

1. No painel de navegação esquerdo, clique em **STORAGE > Storage VMs**.
2. No menu **VIEW**, selecione **Health > All Storage VMs**.

O estado: Todas as VMs de armazenamento é exibido.

3. Clique em **Filter** para visualizar uma das seguintes VMs de armazenamento.

Para ver	Valor do filtro
VMs de armazenamento protegidas	Função de proteção é protegida
VMs de armazenamento desprotegidas	A função de proteção é desprotegida



Você não pode visualizar as VMs de storage protegidas e não protegidas ao mesmo tempo. Você precisará limpar o filtro existente para reaplicar uma nova opção de filtro.

4. Clique em **Apply Filter** (aplicar filtro).

A visualização não salva exibe todas as VMs de storage protegidas ou desprotegidas pela recuperação de desastres da VM de storage com base nas seleções de filtros.

## Noções básicas sobre associações de VM de armazenamento

Associações de máquina virtual de armazenamento (VM de armazenamento) são mapeamentos de uma VM de armazenamento de origem para uma VM de armazenamento de destino que são usados por aplicativos parceiros para seleção de recursos e provisionamento de volume secundário.

Associações são criadas entre uma VM de armazenamento de origem e uma VM de armazenamento de destino, independentemente de a VM de armazenamento de destino ser um destino secundário ou um destino terciário. Você não pode usar uma VM de armazenamento de destino secundário como fonte para criar uma associação com uma VM de armazenamento de destino terciário.

Como Administrador de aplicativo ou Administrador de armazenamento, você pode visualizar as associações de VM de armazenamento em seu ambiente na página **proteção > associações de VM de armazenamento**.

Você pode associar SVMs de três maneiras:

- **Associar qualquer VM de armazenamento:** Você pode criar uma associação entre qualquer VM de armazenamento de origem primária e um ou mais SVMs de destino. Isso significa que todos os SVMs existentes que atualmente exigem proteção, bem como quaisquer SVMs criadas no futuro, estão associados aos SVMs de destino especificados. Por exemplo, você pode querer que aplicativos de várias fontes diferentes em locais diferentes sejam copiados para um ou mais SVMs de destino em um local.
- **Associar uma VM de armazenamento específica:** Você pode criar uma associação entre uma VM de armazenamento de origem específica e um ou mais SVMs de destino específicas. Por exemplo, se você estiver fornecendo serviços de armazenamento para muitos clientes cujos dados devem ser separados um do outro, você pode escolher essa opção para associar uma VM de armazenamento de origem específica a uma VM de armazenamento de destino específica atribuída apenas a esse cliente.
- **Associar a uma VM de armazenamento externo:** Você pode criar uma associação entre uma VM de armazenamento de origem e um volume flexível externo de uma VM de armazenamento de destino.

### Crie associações de VM de armazenamento

O assistente criar associações de máquinas virtuais de armazenamento permite que aplicativos de proteção de parceiros associem uma VM de armazenamento de origem a uma VM de armazenamento de destino para uso com relacionamentos SnapMirror e SnapVault. Os aplicativos de parceiros usam essas associações no momento do provisionamento inicial de volumes de destino para determinar quais recursos selecionar.dd

#### Antes de começar

- A VM de storage que você está associando já deve existir.
- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Para qualquer VM de armazenamento de origem e tipo de relacionamento, você pode escolher apenas uma VM de armazenamento de destino em cada cluster de destino.

Alterar associações usando as funções delete e create afeta apenas operações futuras de provisionamento. Ele não move volumes de destino existentes.

## Passos

1. No painel de navegação esquerdo, clique em **proteção > associações de VM de armazenamento**.
2. Na página **associações de VM de armazenamento**, clique em **criar**.

O assistente **Create Storage Virtual Machine Associations** é iniciado.

3. Selecione uma das seguintes fontes:

- **\* Qualquer \***

Escolha essa opção quando quiser criar uma associação entre qualquer fonte de VM de storage primário para uma ou mais VM de armazenamento de destino. Isso significa que todas as VMs de storage existentes que atualmente exigem proteção, bem como qualquer VM de storage criada no futuro, estão associadas à VM de storage de destino especificada. Por exemplo, você pode querer que aplicativos de várias fontes diferentes em locais diferentes façam backup de uma ou mais VM de armazenamento de destino em um local.

- **Single**

Escolha esta opção quando quiser selecionar uma VM de armazenamento de origem específica associada a uma ou mais VM de armazenamento de destino. Por exemplo, se você estiver fornecendo serviços de armazenamento para muitos clientes cujos dados devem ser separados um do outro, escolha esta opção para associar uma fonte de VM de armazenamento específica a um destino de VM de armazenamento específico atribuído apenas a esse cliente.

- **Nenhuma (externa)**

Escolha essa opção quando quiser criar uma associação entre uma VM de armazenamento de origem e um volume flexível externo de uma VM de armazenamento de destino.

4. Selecione um ou ambos os tipos de relação de proteção que deseja criar:

- **SnapMirror**
- **SnapVault**

5. Clique em **seguinte**.
6. Selecione um ou mais destinos de proteção da VM de storage.
7. Clique em **Finish**.

## Excluir associações de VM de armazenamento

Você pode excluir associações de VM de armazenamento para aplicativos parceiros para remover a relação de provisionamento secundário entre VM de armazenamento de origem e destino; por exemplo, você pode fazer isso quando a VM de armazenamento de destino estiver cheia e desejar criar novas associações de proteção de VM de armazenamento.

### Antes de começar

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

O botão **Delete** é desativado até que pelo menos uma associação de VM de armazenamento seja selecionada. Alterar associações usando as funções excluir e criar afeta apenas operações futuras de

provisionamento; ele não move volumes de destino existentes.

### Passos

1. No painel de navegação esquerdo, clique em **proteção > associações de VM de armazenamento**.
2. Selecione pelo menos uma associação de VM de armazenamento.

O botão **Delete** está ativado.

3. Clique em **Excluir**.

É apresentada uma caixa de diálogo de aviso.

4. Clique em **Yes** para continuar.

A associação de VM de armazenamento selecionada é removida da lista.

## Requisitos de SVM e pool de recursos para dar suporte a serviços de storage

Você garante a conformidade nas aplicações de parceiros se observar alguns requisitos de associação SVM e pool de recursos específicos aos serviços de storage: Por exemplo, quando você associa SVM e cria pools de recursos no Unified Manager a fim de dar suporte a uma topologia de proteção em um serviço de storage fornecido por uma aplicação de parceiro.

Algumas aplicações fazem parceria com o servidor do Unified Manager para fornecer serviços que configuram e executam automaticamente proteção de backup SnapMirror ou SnapVault entre volumes de origem e volumes de proteção em locais secundários ou terciários. Para dar suporte a esses serviços de storage de proteção, use o Unified Manager para configurar as associações e os pools de recursos necessários à SVM.

Para oferecer suporte à proteção de salto único ou em cascata do serviço de storage, incluindo replicação de uma fonte SnapMirror ou volume primário SnapVault para o SnapMirror de destino ou para volumes de backup do SnapVault que residem em locais secundários ou terciários, observe os seguintes requisitos:

- As associações do SVM devem ser configuradas entre o SVM que contém a fonte SnapMirror ou o volume primário SnapVault e qualquer SVM em que residam um volume secundário ou um volume terciário.
    - Por exemplo, para oferecer suporte a uma topologia de proteção na qual o volume de origem vol\_A reside no SVM\_1 3, e o volume de destino secundário vol\_B do SnapMirror reside no SVM\_2, e o volume de backup terciário SnapVault vol\_C reside no SVM\_3, você deve usar a IU da Web do Unified Manager para configurar uma associação de SnapMirror entre SVM\_1 e SVM\_2 e uma associação de backup do SnapVault entre SVM\_1.
- Neste exemplo, qualquer associação SnapMirror ou associação de backup do SnapVault entre SVM\_2 e SVM\_3 não é necessária e não é usada.
- Para dar suporte a uma topologia de proteção na qual o volume de origem vol\_A e o volume de destino do SnapMirror vol\_B estejam na SVM\_1, você deve configurar uma associação SnapMirror entre o SVM\_1 e o SVM\_1.
- Os pools de recursos devem incluir recursos agregados de cluster disponíveis para os SVMs associados.

Você configura pools de recursos por meio da IU da Web do Unified Manager e atribui, por meio da aplicação de parceiro, os nós de destino secundário e terciário.

## Quais são os empregos

Um trabalho é uma série de tarefas que você pode monitorar usando o Unified Manager. A visualização de trabalhos e respectivas tarefas associadas permite-lhe determinar se foram concluídos com êxito.

As tarefas são iniciadas quando você cria relações SnapMirror e SnapVault, quando você executa qualquer operação de relacionamento (quebrar, editar, quiesce, remover, retomar, ressincronizar e reverter a ressincronização), quando você executa tarefas de restauração de dados, quando você faz login em um cluster, e assim por diante.

Quando inicia um trabalho, pode utilizar a página trabalhos e a página Detalhes do trabalho para monitorizar o trabalho e o progresso das tarefas associadas.

## Tarefas de monitorização

Pode utilizar a página trabalhos para monitorizar o estado da tarefa e para ver as propriedades da tarefa, tais como tipo de serviço de armazenamento, estado, tempo de envio e tempo de conclusão, para determinar se uma tarefa foi concluída com êxito ou não.

### Antes de começar

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

### Passos

1. No painel de navegação esquerdo, clique em **proteção > empregos**.

É apresentada a página trabalhos.

2. Exiba a coluna **Estado** para determinar o status dos trabalhos atualmente em execução.
3. Clique no nome de um trabalho para ver detalhes sobre esse trabalho específico.

É apresentada a página Detalhes do trabalho.

## Exibindo detalhes do trabalho

Depois de iniciar um trabalho, pode monitorizar o seu progresso a partir da página Detalhes do trabalho e monitorizar as tarefas associadas relativamente a possíveis erros.

### Antes de começar

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

### Passos

1. No painel de navegação esquerdo, clique em **proteção > empregos**.
2. Na página trabalhos, clique no nome de um trabalho na coluna **Nome** para exibir a lista de tarefas associadas ao trabalho.
3. Clique em uma tarefa para exibir informações adicionais no painel **Detalhes da tarefa** e no painel **mensagens da tarefa** à direita da lista de tarefas.

## A abortar trabalhos

Pode utilizar a página trabalhos para abortar um trabalho se estiver a demorar demasiado tempo a terminar, se encontrar demasiados erros ou se já não for necessário. Só é possível cancelar um trabalho se o seu estado e tipo permitir. Pode cancelar qualquer trabalho em execução.

### Antes de começar

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

### Passos

1. No painel de navegação esquerdo, clique em **proteção > empregos**.
2. Na lista de trabalhos, selecione um trabalho e, em seguida, clique em **Abortar**.
3. No prompt de confirmação, clique em **Yes** para cancelar o trabalho selecionado.

## Tentar novamente um trabalho de proteção com falha

Depois de tomar medidas para corrigir um trabalho de proteção com falha, você pode usar **Repetir** para executar o trabalho novamente. Tentar novamente um trabalho cria um novo trabalho usando o ID do trabalho original.

### Antes de começar

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

Você pode tentar novamente apenas um trabalho com falha de cada vez. Selecionar mais de um trabalho desativa o botão **Repetir**. Apenas os trabalhos do tipo Configuração de proteção e operação de relação de proteção podem ser tentados novamente.

### Passos

1. No painel de navegação esquerdo, clique em **proteção > empregos**.
2. Na lista de trabalhos, selecione uma única tarefa de tipo de operação de relação de proteção ou Configuração de proteção com falha.

O botão **Repetir** está ativado.

3. Clique em **Repetir**.

O trabalho é reiniciado.

## Descrição das janelas de relacionamentos de proteção e caixas de diálogo

Você pode visualizar e gerenciar detalhes relacionados à proteção, como pools de recursos, associações de SVM e tarefas de proteção. Você pode usar a página limites de integridade apropriados para configurar valores de limites globais de integridade para agregados, volumes e relacionamentos.

### Página de pools de recursos

A página pools de recursos exibe pools de recursos existentes e seus membros e

permite criar, monitorar e gerenciar pools de recursos para fins de provisionamento.

#### Botões de comando

Os botões de comando permitem executar as seguintes tarefas:

- **Criar**

Inicia a caixa de diálogo criar pool de recursos, que você pode usar para criar pools de recursos.

- **Editar**

Permite editar o nome e a descrição dos pools de recursos criados.

- **Excluir**

Permite excluir um ou mais pools de recursos.

#### Lista de pools de recursos

A lista pools de recursos exibe (em formato tabular) as propriedades dos pools de recursos existentes.

- **Pool de recursos**

Exibe o nome do pool de recursos.

- **Descrição**

Descreve o pool de recursos.

- **Tipo SnapLock**

Exibe o tipo SnapLock que está sendo usado pelos agregados no pool de recursos. Os valores válidos para o tipo SnapLock são Compliance, Enterprise e Non-SnapLock. Um pool de recursos pode conter agregados de apenas um tipo SnapLock.

- \* Capacidade total\*

Exibe a capacidade total (em MB, GB e assim por diante) do pool de recursos.

- \* Capacidade utilizada\*

Exibe a quantidade de espaço (em MB, GB e assim por diante) que é usada no pool de recursos.

- **Capacidade disponível**

Exibe a quantidade de espaço (em MB, GB e assim por diante) disponível no pool de recursos.

- **% Usados**

Exibe a porcentagem de espaço usada no pool de recursos.

#### Botões de comando da lista de membros

Os botões de comando Lista de membros permitem executar as seguintes tarefas:

- **Adicionar**

Permite adicionar membros ao pool de recursos.

- **Excluir**

Permite excluir um ou mais membros do pool de recursos.

### Lista de membros

A lista Membros exibe (em formato tabular) os membros do pool de recursos e suas propriedades quando um pool de recursos é selecionado.

- **Status**

Exibe o status atual do agregado membro. O status pode ser crítico (❌), erro (⚠️), Aviso (⚠️) ou normal (✅).

- **Nome agregado**

Exibe o nome do agregado membro.

- **Estado**

Exibe o estado atual do agregado, que pode ser um dos seguintes:

- Offline

Acesso de leitura ou gravação não é permitido.

- Online

O acesso de leitura e gravação aos volumes que estão hospedados neste agregado é permitido.

- Restrito

Operações limitadas (como reconstrução de paridade) são permitidas, mas o acesso aos dados não é permitido.

- A criar

O agregado está sendo criado.

- Destruindo

O agregado está sendo destruído.

- Falha

O agregado não pode ser colocado online.

- Congelado

O agregado não está (temporariamente) atendendo solicitações.



- Inconsistente

O agregado foi marcado como corrompido; você deve entrar em Contato com o suporte técnico.

- Ferro restrito

As ferramentas de diagnóstico não podem ser executadas no agregado.

- Montagem

O agregado está em processo de montagem.

- Parcial

Pelo menos um disco foi encontrado para o agregado, mas dois ou mais discos estão faltando.

- Quiescing

O agregado está sendo silenciado.

- Quiesced

O agregado é aquiesced.

- Revertido

A reversão de um agregado é concluída.

- Desmontado

O agregado foi desmontado.

- Desmontagem

O agregado está sendo colocado off-line.

- Desconhecido

O agregado é descoberto, mas as informações agregadas ainda não são recuperadas pelo servidor do Unified Manager.

Por padrão, essa coluna está oculta.

- **Cluster**

Exibe o nome do cluster ao qual o agregado pertence.

- **Nó**

Exibe o nome do nó no qual o agregado reside.

- \* Capacidade total\*

Exibe a capacidade total (em MB, GB e assim por diante) do agregado.

- \* Capacidade utilizada\*

Exibe a quantidade de espaço (em MB, GB e assim por diante) que é usada no agregado.

- **Capacidade disponível**

Exibe a quantidade de espaço (em MB, GB e assim por diante) que está disponível no agregado.

- **% Usados**

Exibe a porcentagem de espaço que é usado no agregado.

- **Tipo de disco**

Exibe o tipo de configuração RAID, que pode ser um dos seguintes:

- RAID0: Todos os grupos RAID são do tipo RAID0.
- RAID4: Todos os grupos RAID são do tipo RAID4.
- RAID-DP: Todos os grupos RAID são do tipo RAID-DP.
- RAID-TEC: Todos os grupos RAID são do tipo RAID-TEC.
- RAID misto: O agregado contém grupos RAID de diferentes tipos de RAID (RAID0, RAID4, RAID-DP e RAID-TEC). Por padrão, essa coluna está oculta.

## **Caixa de diálogo criar pool de recursos**

Você pode usar a caixa de diálogo criar pool de recursos para nomear e descrever um novo pool de recursos e adicionar agregados e excluir agregados desse pool de recursos.

### **Nome do conjunto de recursos**

As caixas de texto permitem adicionar as seguintes informações para criar um pool de recursos:

Permite especificar um nome de pool de recursos.

### **Descrição**

Permite descrever um pool de recursos.

### **Membros**

Exibe os membros do pool de recursos. Você também pode adicionar e excluir membros.

### **Botões de comando**

Os botões de comando permitem executar as seguintes tarefas:

- **Adicionar**

Abre a caixa de diálogo agregados para que você possa adicionar agregados de um cluster específico ao pool de recursos. É possível adicionar agregados de clusters diferentes, mas os mesmos agregados não podem ser adicionados a mais de um pool de recursos.

- **Remover**

Permite remover agregados selecionados do pool de recursos.

- **Criar**

Cria o pool de recursos. Este botão não está ativado até que as informações tenham sido introduzidas nos campos Nome do conjunto de recursos ou Descrição.

- **Cancelar**

Descarta as alterações e fecha a caixa de diálogo criar pool de recursos.

### **Caixa de diálogo Editar pool de recursos**

Você pode usar a caixa de diálogo Editar pool de recursos para alterar o nome e a descrição de um pool de recursos existente. Por exemplo, se o nome e a descrição originais forem imprecisos ou incorretos, você pode alterá-los para que sejam mais precisos.

#### **Caixas de texto**

As caixas de texto permitem alterar as seguintes informações para o pool de recursos selecionado:

- **Nome do pool de recursos**

Permite-lhe introduzir um novo nome.

- **Descrição**

Permite-lhe introduzir uma nova descrição.

#### **Botões de comando**

Os botões de comando permitem executar as seguintes tarefas:

- **Guardar**

Salva as alterações no nome e na descrição do pool de recursos.

- **Cancelar**

Descarta as alterações e fecha a caixa de diálogo Editar pool de recursos.

### **Caixa de diálogo agregados**

Você pode usar a caixa de diálogo agregados para selecionar os agregados que deseja adicionar ao pool de recursos.

#### **Botões de comando**

Os botões de comando permitem executar as seguintes tarefas:

- **Adicionar**

Adiciona os agregados selecionados ao pool de recursos. O botão Adicionar não está ativado até que pelo menos um agregado seja selecionado.

- **Cancelar**

Descarta as alterações e fecha a caixa de diálogo agregados.

### Lista de agregados

A lista de agregados exibe (em formato tabular) os nomes e propriedades dos agregados monitorados.

- **Status**

Apresenta o estado atual de um volume. O status pode ser crítico (❌), erro (⚠️), Aviso (⚠️) ou normal (✅).

Você pode mover o ponteiro sobre o status para exibir mais informações sobre o evento ou eventos gerados para o volume.

- **Nome agregado**

Exibe o nome do agregado.

- **Estado**

Exibe o estado atual do agregado, que pode ser um dos seguintes:

- Offline

Acesso de leitura ou gravação não é permitido.

- Restrito

Operações limitadas (como reconstrução de paridade) são permitidas, mas o acesso aos dados não é permitido.

- Online

O acesso de leitura e gravação aos volumes que estão hospedados neste agregado é permitido.

- A criar

O agregado está sendo criado.

- Destruindo

O agregado está sendo destruído.

- Falha

O agregado não pode ser colocado online.

- Congelado

O agregado não está (temporariamente) atendendo solicitações.

- Inconsistente

O agregado foi marcado como corrompido; você deve entrar em Contato com o suporte técnico.

- Ferro restrito

As ferramentas de diagnóstico não podem ser executadas no agregado.

- Montagem

O agregado está em processo de montagem.

- Parcial

Pelo menos um disco foi encontrado para o agregado, mas dois ou mais discos estão faltando.

- Quiescing

O agregado está sendo silenciado.

- Quiesced

O agregado é aquiesced.

- Revertido

A reversão de um agregado é concluída.

- Desmontado

O agregado está offline.

- Desmontagem

O agregado está sendo colocado off-line.

- Desconhecido

O agregado é descoberto, mas as informações agregadas ainda não são recuperadas pelo servidor do Unified Manager.

- **Cluster**

Exibe o nome do cluster no qual o agregado reside.

- **Nó**

Exibe o nome do controlador de armazenamento que contém o agregado.

- \* Capacidade total\*

Exibe o tamanho total dos dados (em MB, GB e assim por diante) do agregado. Por padrão, essa coluna está oculta.

- **Capacidade comprometida**

Exibe o espaço total (em MB, GB e assim por diante) comprometido para todos os volumes no agregado. Por padrão, essa coluna está oculta.

- **\* Capacidade utilizada\***

Exibe a quantidade de espaço (em MB, GB e assim por diante) que é usada no agregado.

- **Capacidade disponível**

Exibe a quantidade de espaço (em MB, GB e assim por diante) disponível para dados no agregado. Por padrão, essa coluna está oculta.

- **% Disponível**

Exibe a porcentagem de espaço disponível para os dados no agregado. Por padrão, essa coluna está oculta.

- **% Usados**

Exibe a porcentagem de espaço que é usada pelos dados no agregado.

- **Tipo RAID**

Exibe o tipo RAID do volume selecionado. O tipo RAID pode ser RAID0, RAID4, RAID-DP, RAID-TEC ou RAID misto.

## Página de trabalhos

A página trabalhos permite visualizar o estado atual e outras informações sobre todos os trabalhos de proteção de aplicativos de parceiros que estão sendo executados no momento, bem como os trabalhos concluídos. Pode utilizar estas informações para ver quais trabalhos ainda estão a ser executados e se um trabalho foi bem-sucedido ou falhou.

### Botões de comando

Os botões de comando permitem executar as seguintes tarefas:

- **\* Cancelar\***

Aborta o trabalho selecionado. Esta opção só está disponível se o trabalho selecionado estiver em execução.

- **Repetir**

Reinicia um trabalho com falha do tipo Configuração de proteção ou operação de relação de proteção. Você pode tentar novamente apenas um trabalho com falha de cada vez. Se for selecionado mais de um trabalho com falha, o botão **Repetir** é desativado. Não é possível tentar novamente trabalhos de serviço de armazenamento falhados.

- **Atualizar**

Atualiza a lista de trabalhos e as informações associadas a eles.

## Lista de trabalhos

A lista trabalhos apresenta, em formato tabular, uma lista dos trabalhos em curso. Por predefinição, a lista apresenta apenas os trabalhos gerados na semana passada. Pode utilizar a ordenação e a filtragem de colunas para personalizar os trabalhos apresentados.

- **Status**

Apresenta o estado atual de um trabalho. O status pode ser erro () ou normal (.

- **ID do trabalho**

Apresenta o número de identificação do trabalho. Por padrão, essa coluna está oculta.

O número de identificação do trabalho é único e é atribuído pelo servidor quando inicia o trabalho. Pode procurar um trabalho específico introduzindo o número de identificação do trabalho na caixa de texto fornecida pelo filtro de coluna.

- **Nome**

Apresenta o nome do trabalho.

- **Tipo**

Apresenta o tipo de trabalho. Os tipos de tarefa são os seguintes:

- **Aquisição de cluster**

Um trabalho de automação do fluxo de trabalho está redescobrimo um cluster.

- **Configuração de proteção**

Um trabalho de proteção está iniciando fluxos de trabalho de automação do fluxo de trabalho, como cronogramas cron, criação de políticas do SnapMirror e assim por diante.

- \* Operação de relacionamento de proteção\*

Um trabalho de proteção está executando operações do SnapMirror.

- \* Cadeia de fluxo de trabalho de proteção\*

Um trabalho de automação do fluxo de trabalho está executando vários fluxos de trabalho.

- **Restaurar**

Um trabalho de restauração está em execução.

- **Limpeza**

O trabalho está limpando artefatos dos membros do serviço de armazenamento que não são mais necessários para fins de restauração.

- **Em conformidade**

O trabalho está verificando a configuração dos membros do serviço de armazenamento para garantir que eles estão em conformidade.

- **Destrua**

O trabalho está destruindo um serviço de armazenamento.

- **Importação**

A tarefa está importando objetos de armazenamento não gerenciados para um serviço de armazenamento existente.

- **Modificar**

A tarefa está modificando atributos de um serviço de armazenamento existente.

- **Subscribe**

O trabalho está assinando membros de um serviço de armazenamento.

- **Cancelar inscrição**

O trabalho está descadastrando membros de um serviço de armazenamento.

- **Atualização**

Um trabalho de atualização de proteção está em execução.

- **Configuração WFA**

Um trabalho do Workflow Automation está enviando credenciais de cluster e sincronizando caches de banco de dados.

- **Estado**

Apresenta o estado em execução do trabalho. As opções de estado são as seguintes:

- **Abortado**

O trabalho foi abortado.

- **Aborting**

O trabalho está em processo de abortar.

- **Concluído**

O trabalho terminou.

- **Running**

O trabalho está em execução.

- **Tempo de envio**

Exibe a hora em que o trabalho foi enviado.

- **Duração**



Exibe o tempo que o trabalho levou para concluir. Esta coluna é apresentada por predefinição.

- **Tempo completo**

Apresenta a hora em que o trabalho terminou. Por padrão, essa coluna está oculta.

## **Página de detalhes do trabalho**

A página Detalhes do trabalho permite exibir status e outras informações sobre tarefas específicas de trabalho de proteção que estão em execução, que estão em fila ou que foram concluídas. Você pode usar essas informações para monitorar o progresso do trabalho de proteção e solucionar falhas de trabalho.

### **Resumo do trabalho**

O resumo do trabalho apresenta as seguintes informações:

- ID do trabalho
- Tipo
- Estado
- Tempo de envio
- Hora concluída
- Duração

### **Botões de comando**

Os botões de comando permitem executar as seguintes tarefas:

- **Atualizar**

Atualiza a lista de tarefas e as propriedades associadas a cada tarefa.

- **Ver trabalhos**

Retorna para a página trabalhos.

### **Lista de tarefas do trabalho**

A lista tarefas da tarefa exibe em uma tabela todas as tarefas associadas a uma tarefa específica e as propriedades relacionadas a cada tarefa.

- **Hora de início**

Apresenta o dia e a hora em que a tarefa foi iniciada. Por padrão, as tarefas mais recentes são exibidas na parte superior da coluna e as tarefas mais antigas são exibidas na parte inferior.

- **Tipo**

Exibe o tipo de tarefa.

- **Estado**

O estado de uma determinada tarefa:

- **Concluído**

A tarefa terminou.

- **Em fila**

A tarefa está prestes a ser executada.

- **Running**

A tarefa está em execução.

- \* **Espera\***

Um trabalho foi enviado e algumas tarefas associadas estão aguardando para serem enfileiradas e executadas.

- **Status**

Apresenta o estado da tarefa:

- **Erro (🚫)**

A tarefa falhou.

- **Normal (✅)**

A tarefa foi bem-sucedida.

- **Pulado (🔄)**

Uma tarefa falhou, resultando em tarefas subsequentes sendo ignoradas.

- **Duração**

Apresenta o tempo decorrido desde o início da tarefa.

- **Tempo completo**

Exibe a hora em que a tarefa foi concluída. Por padrão, essa coluna está oculta.

- **ID da tarefa**

Apresenta o GUID que identifica uma tarefa individual para um trabalho. A coluna pode ser classificada e filtrada. Por padrão, essa coluna está oculta.

- **Ordem de dependência**

Exibe um número inteiro representando a sequência de tarefas em um gráfico, com zero sendo atribuído à primeira tarefa. Por padrão, essa coluna está oculta.

- **Painel Detalhes da tarefa**

Apresenta informações adicionais sobre cada tarefa de trabalho, incluindo o nome da tarefa, a descrição

da tarefa e, se a tarefa falhar, um motivo para a falha.

- **Painel de mensagens da tarefa**

Exibe mensagens específicas para a tarefa selecionada. As mensagens podem incluir um motivo para o erro e sugestões para resolvê-lo. Nem todas as tarefas exibem mensagens de tarefa.

## **Caixa de diálogo Configurações secundárias avançadas**

Você pode usar a caixa de diálogo Configurações secundárias avançadas para habilitar a replicação flexível de versão, backup de várias cópias e configurações relacionadas ao espaço em um volume secundário. Você pode usar a caixa de diálogo Configurações secundárias avançadas quando quiser alterar Ativar ou desativar as configurações atuais.

As configurações relacionadas ao espaço maximizam a quantidade de dados armazenados, incluindo: Deduplicação, compressão de dados, crescimento automático e garantia de espaço.

A caixa de diálogo inclui os seguintes campos:

- **Ativar replicação flexível de versão**

Habilita o SnapMirror com replicação flexível da versão. A replicação flexível da versão permite a proteção SnapMirror de um volume de origem, mesmo que o volume de destino esteja sendo executado em uma versão anterior do ONTAP do que a do volume de origem.

- Ativar cópia de segurança

Se a replicação flexível da versão estiver ativada, também permitirá que várias cópias Snapshot dos dados de origem do SnapMirror sejam transferidas e retidas no destino do SnapMirror.

- **Ativar deduplicação**

Habilita a deduplicação no volume secundário em uma relação do SnapVault, para que blocos de dados duplicados sejam eliminados para alcançar economia de espaço. Você pode usar a deduplicação quando a economia de espaço é de pelo menos 10% e quando a taxa de substituição de dados não é rápida. A deduplicação geralmente é usada para ambientes virtualizados, compartilhamentos de arquivos e dados de backup. Esta definição está desativada por predefinição. Quando ativada, esta operação é iniciada após cada transferência.

- Ative a compressão

Permite a compactação de dados transparente. Você pode usar a compactação quando a economia de espaço for de pelo menos 10%, quando a sobrecarga potencial for aceitável e quando houver recursos suficientes do sistema para que a compactação seja concluída durante horas que não sejam de pico. Em um relacionamento SnapVault, essa configuração é desativada por padrão. A compactação está disponível somente quando a deduplicação está selecionada.

- Comprimir em linha

Permite economia imediata de espaço comprimindo dados antes de gravar dados no disco. Você pode usar a compactação in-line quando o sistema não tiver mais de 50% de utilização durante o horário de pico e quando o sistema puder acomodar novas gravações e CPU adicional durante o horário de pico. Esta configuração está disponível somente quando ""Ativar compressão"" está selecionado.

- **Ativar crescimento automático**

Permite que você aumente automaticamente o volume de destino quando a porcentagem de espaço livre estiver abaixo do limite especificado, contanto que o espaço esteja disponível no agregado associado.

- \* Tamanho máximo\*

Define a porcentagem máxima para a qual um volume pode crescer. O padrão é 20% maior do que o tamanho do volume de origem. Um volume não cresce automaticamente se o tamanho atual for maior ou igual à porcentagem máxima de crescimento automático. Este campo é ativado apenas quando a definição de crescimento automático está ativada.

- \* Tamanho de incremento\*

Especifica o incremento percentual pelo qual o volume cresce automaticamente antes de atingir a porcentagem máxima do volume de origem.

- **Garantia de espaço**

Garante que espaço suficiente seja alocado no volume secundário para que as transferências de dados sejam sempre bem-sucedidas. A configuração de garantia de espaço pode ser uma das seguintes:

- Ficheiro
- Volume
- Por exemplo, você pode ter um volume de 200 GB que contém arquivos totalizando 50 GB; no entanto, esses arquivos contêm apenas 10 GB de dados. A garantia de volume aloca 200 GB para o volume de destino, independentemente do conteúdo na origem. Garantia de arquivo aloca 50 GB para garantir que espaço suficiente seja reservado para arquivos na origem; selecionar nenhum neste cenário significa que apenas 10 GB é alocado no destino para o espaço real usado pelos dados de arquivo na origem.

A garantia de espaço é definida como volume por padrão.

### Botões de comando

Os botões de comando permitem executar as seguintes tarefas:

- **Aplicar**

Salva as configurações de eficiência selecionadas e as aplica quando você clica em **Apply** na caixa de diálogo Configurar proteção.

- **Cancelar**

Descarta suas seleções e fecha a caixa de diálogo Configurações avançadas de destino.

### Caixa de diálogo Configurações avançadas de destino

Você pode usar a caixa de diálogo Configurações avançadas de destino para ativar as configurações de garantia de espaço em um volume de destino. Você pode selecionar configurações avançadas quando a garantia de espaço estiver desativada na origem, mas deseja que ela seja ativada no destino. As configurações de deduplicação, compactação e crescimento automático em um relacionamento SnapMirror são herdadas

do volume de origem e não podem ser alteradas.

### Garantia de espaço

Garante que espaço suficiente seja alocado no volume de destino para que as transferências de dados sejam sempre bem-sucedidas. A configuração de garantia de espaço pode ser uma das seguintes:

- Ficheiro
- Volume
- Nenhum

Por exemplo, você pode ter um volume de 200 GB que contém arquivos totalizando 50 GB; no entanto, esses arquivos contêm apenas 10 GB de dados. A garantia de volume aloca 200 GB para o volume de destino, independentemente do conteúdo na origem. Garantia de arquivo aloca 50 GB para garantir que espaço suficiente seja reservado para arquivos de origem no destino; selecionar **nenhum** neste cenário significa que apenas 10 GB é alocado no destino para o espaço real usado pelos dados de arquivo na origem.

A garantia de espaço é definida como volume por padrão.

### Caixa de diálogo Restaurar

Você pode usar a caixa de diálogo Restaurar para restaurar dados para um volume de uma cópia Snapshot específica.

#### Restaurar de

A área Restaurar de permite especificar de onde deseja restaurar dados.

- **Volume**

Especifica o volume a partir do qual você deseja restaurar dados. Por padrão, o volume no qual você iniciou a ação de restauração é selecionado. Você pode selecionar um volume diferente na lista suspensa que contém todos os volumes com relações de proteção para o volume no qual você iniciou a ação de restauração.

- **Cópia Snapshot**

Especifica qual cópia Snapshot você deseja usar para restaurar dados. Por padrão, a cópia Snapshot mais recente é selecionada. Você também pode selecionar uma cópia Snapshot diferente na lista suspensa. A lista de cópias instantâneas muda de acordo com o volume selecionado.

- **Lista o máximo de 995 arquivos e diretórios**


Por padrão, um máximo de 995 objetos são mostrados na lista. Você pode desmarcar essa caixa de seleção se quiser exibir todos os objetos dentro do volume selecionado. Esta operação pode demorar algum tempo se o número de itens for muito grande.

#### Selecione itens para restaurar

A área Selecionar itens para restaurar permite selecionar o volume inteiro ou arquivos e pastas específicos que você deseja restaurar. Pode selecionar um máximo de 10 ficheiros, pastas ou uma combinação de ambos. Quando o número máximo de itens é selecionado, as caixas de seleção de item são desativadas.

- **Campo caminho**

Exibe o caminho para os dados que deseja restaurar. Você pode navegar para a pasta e os arquivos que deseja restaurar ou digitar o caminho. Este campo fica vazio até selecionar ou introduzir um caminho.

Clicar  depois de ter escolhido um caminho o move para um nível acima na estrutura de diretórios.

- **Lista de pastas e arquivos**

Apresenta o conteúdo do caminho introduzido. Por padrão, a pasta raiz é exibida inicialmente. Clicar em um nome de pasta exibe o conteúdo da pasta.

Você pode selecionar itens para restaurar da seguinte forma:

- Quando você insere o caminho com um nome de arquivo específico especificado no campo caminho, o arquivo especificado é exibido nas pastas e arquivos.
- Quando você insere um caminho sem especificar um arquivo específico, o conteúdo da pasta é exibido na lista pastas e arquivos e você pode selecionar até 10 arquivos, pastas ou uma combinação de ambos para restaurar.

Se uma pasta contiver mais de 995 itens, é apresentada uma mensagem para indicar que existem demasiados itens a apresentar e, se prosseguir com a operação, todos os itens da pasta especificada são restaurados. Você pode desmarcar a caixa de seleção "List maximum of 995 files and directories" se quiser exibir todos os objetos dentro do volume selecionado.



Não é possível restaurar fluxos de ficheiros NTFS.

### Restaurar para

A área Restaurar para permite especificar onde deseja restaurar os dados.

- **Localização original em volume\_Name**

Restaura os dados selecionados para o diretório na origem a partir do qual os dados foram originalmente copiados.

- **Localização alternativa**

Restaura os dados selecionados para um novo local:

- Restaurar caminho

Especifica um caminho alternativo para restaurar os dados selecionados. O caminho já deve existir. Você pode usar o botão **Procurar** para navegar até o local onde deseja que os dados sejam restaurados ou pode inserir o caminho manualmente usando o cluster de formatos://svm/volume/caminho.

- Preservar a hierarquia de diretórios

Quando marcada, preserva a estrutura do arquivo ou diretório original. Por exemplo, se a origem for /A/B/C/myFile.txt e o destino for /X/Y/Z, o Unified Manager restaura os dados usando a seguinte estrutura de diretórios no destino: /X/Y/Z/A/B/C/myfile.txt.

## Botões de comando

Os botões de comando permitem executar as seguintes tarefas:

- **Cancelar**

Descarta suas seleções e fecha a caixa de diálogo Restaurar.

- **Restaurar**

Aplica suas seleções e inicia o processo de restauração.

## Caixa de diálogo Procurar diretórios

Você pode usar a caixa de diálogo Procurar diretórios quando quiser restaurar dados para um diretório em um cluster e SVM diferente da origem original. O cluster de origem e o volume originais são selecionados por padrão.

A caixa de diálogo Procurar diretórios permite selecionar o cluster, SVM, volume e caminho do diretório para o qual você deseja que os dados sejam restaurados.

- **Cluster**

Lista os destinos de cluster disponíveis para os quais pode restaurar. Por predefinição, é selecionado o cluster do volume de origem original.

- **Lista suspensa SVM**

Lista o SVM disponível disponível para o cluster selecionado. Por padrão, o SVM do volume de origem original é selecionado.

- **Volume**

Lista todos os volumes de leitura/gravação em um SVM selecionado. Você pode filtrar os volumes por nome e por espaço disponível. O volume com mais espaço é listado primeiro, e assim por diante, em ordem decrescente. Por predefinição, o volume de origem original é selecionado.

- \* Caixa de texto caminho do arquivo\*

Permite que você digite o caminho do arquivo para o qual deseja que os dados sejam restaurados. O caminho inserido já deve existir.

- **Nome**

Apresenta os nomes das pastas disponíveis para o volume selecionado. Clicar em uma pasta na lista Nome exibe as subpastas, se houver. Os ficheiros contidos nas pastas não são apresentados. Ao clicar



depois de selecionar uma pasta, você sobe um nível na estrutura de diretórios.

## Botões de comando

Os botões de comando permitem executar as seguintes tarefas:

- **Selecione diretório**

Aplica suas seleções e fecha a caixa de diálogo Procurar diretórios. Se nenhum diretório for selecionado, este botão será desativado.

- **Cancelar**

Descarta suas seleções e fecha a caixa de diálogo Procurar diretórios.

## **Caixa de diálogo Configurar proteção**

Você pode usar a caixa de diálogo Configurar proteção para criar relacionamentos SnapMirror e SnapVault para todos os volumes de leitura, gravação e proteção de dados nos clusters para garantir que os dados em um volume de origem ou volume primário sejam replicados.

### **Separador origem**

- **Vista de topologia**

Exibe uma representação visual da relação que você está criando. A fonte na topologia é realçada por padrão.

- **Informações de origem**

Exibe detalhes sobre os volumes de origem selecionados, incluindo as seguintes informações:

- Nome do cluster de origem
- Nome do SVM de origem
- Tamanho total do volume acumulado

Exibe o tamanho total de todos os volumes de origem selecionados.

- Volume cumulativo usado tamanho

Exibe o volume cumulativo usado para todos os volumes de origem selecionados.

- Volume de origem

Exibe as seguintes informações em uma tabela:

- Volume de origem

Exibe os nomes dos volumes de origem selecionados.

- Tipo

Apresenta o tipo de volume.

- Tipo SnapLock

Apresenta o tipo SnapLock do volume. As opções são Compliance, Enterprise e Non-SnapLock.

- Cópia Snapshot

Exibe a cópia Snapshot usada para a transferência da linha de base. Se o volume de origem for



leitura/gravação, o valor padrão na coluna cópia Snapshot indica que uma nova cópia Snapshot é criada por padrão e usada para a transferência da linha de base. Se o volume de origem for um volume de proteção de dados, o valor padrão na coluna cópia Snapshot indica que nenhuma nova cópia Snapshot foi criada e todas as cópias Snapshot existentes serão transferidas para o destino. Clicar no valor cópia Snapshot exibe uma lista de cópias Snapshot a partir das quais você pode selecionar uma cópia Snapshot existente a ser usada para a transferência da linha de base. Não é possível selecionar uma cópia Snapshot padrão diferente se o tipo de origem for proteção de dados.

## Guia SnapMirror

Permite especificar um cluster de destino, uma máquina virtual de storage (SVM) e um agregado para um relacionamento de proteção, bem como uma convenção de nomenclatura para destinos ao criar um relacionamento com o SnapMirror. Você também pode especificar uma política e uma programação do SnapMirror.

### • Vista de topologia

Exibe uma representação visual da relação que você está criando. O recurso de destino do SnapMirror na topologia é realçado por padrão.

### • Informações de destino

Permite selecionar os recursos de destino para uma relação de proteção:

- Link avançado

Inicia a caixa de diálogo Configurações avançadas de destino quando você estiver criando uma relação do SnapMirror.

- Cluster

Lista os clusters que estão disponíveis como hosts de destino de proteção. Este campo é obrigatório.

- Máquina virtual de storage (SVM)

Lista os SVMs que estão disponíveis no cluster selecionado. É necessário selecionar um cluster antes da lista SVM ser preenchida. Este campo é obrigatório.

- Agregado

Lista os agregados que estão disponíveis no SVM selecionado. Um cluster deve ser selecionado antes que a lista de agregados seja preenchida. Este campo é obrigatório. A lista de agregados exibe as seguintes informações:

- Classificação

Quando vários agregados satisfazem todos os requisitos de um destino, o rank indica a prioridade na qual o agregado é listado, de acordo com as seguintes condições:

- A. Um agregado que está localizado em um nó diferente do nó de volume de origem é preferível para ativar a separação de domínio de falha.
- B. É preferível um agregado em um nó com menos volumes para permitir o balanceamento de carga entre nós em um cluster.

C. Um agregado que tenha mais espaço livre do que outros agregados é preferido para permitir o balanceamento de capacidade. Uma classificação de 1 significa que o agregado é o mais preferido de acordo com os três critérios.

- Nome agregado

Nome do agregado

- Capacidade disponível
- Quantidade de espaço disponível no agregado para dados
- Pool de recursos

Nome do pool de recursos ao qual o agregado pertence

- Convenção de nomenclatura

Especifica a convenção de nomenclatura padrão aplicada ao volume de destino. Você pode aceitar a convenção de nomenclatura fornecida ou criar uma personalizada. A convenção de nomenclatura pode ter os seguintes atributos: %C, %M, %V e %N, onde %C é o nome do cluster, %M é o nome do SVM, %V é o volume de origem e %N é o nome do nó de destino da topologia.

O campo de convenção de nomenclatura é realçado a vermelho se a sua entrada for inválida. Clicar no link "Nome da visualização" exibe uma visualização da convenção de nomenclatura que você inseriu e o texto de visualização é atualizado dinamicamente à medida que você digita uma convenção de nomenclatura no campo de texto. Um sufixo entre 001 e 999 é anexado ao nome de destino quando a relação é criada, substituindo o nnn que é exibido no texto de visualização, com 001 sendo atribuído primeiro, 002 atribuído segundo, e assim por diante.

## • Configurações de relacionamento

Permite especificar a taxa de transferência máxima, a política SnapMirror e a programação que a relação de proteção usa:

- Taxa de transferência máxima

Especifica a taxa máxima na qual os dados são transferidos entre clusters pela rede. Se você optar por não usar uma taxa de transferência máxima, a transferência de linha de base entre relacionamentos é ilimitada.

- Política de SnapMirror

Especifica a política ONTAP SnapMirror para o relacionamento. A predefinição é DPDefault.

- Criar política

Inicia a caixa de diálogo criar política de SnapMirror, que permite criar e usar uma nova política de SnapMirror.

- Programação SnapMirror

Especifica a política ONTAP SnapMirror para o relacionamento. Os horários disponíveis incluem nenhum, 5min, 8hour, diariamente, por hora e semanalmente. O padrão é nenhum, indicando que nenhum agendamento está associado ao relacionamento. Relacionamentos sem agendamentos não têm valores de status de atraso, a menos que pertençam a um serviço de storage.

- Criar Agendamento

Inicia a caixa de diálogo criar Agendamento, que permite criar uma nova agenda SnapMirror.

## Guia SnapVault

Permite especificar um cluster secundário, SVM e agregado para um relacionamento de proteção, bem como uma convenção de nomenclatura para volumes secundários enquanto cria um relacionamento de SnapVault. Você também pode especificar uma política e uma programação do SnapVault.

### • Vista de topologia

Exibe uma representação visual da relação que você está criando. O recurso secundário do SnapVault na topologia é realçado por padrão.

### • Informações secundárias

Permite selecionar os recursos secundários para uma relação de proteção:

- Link avançado

Inicia a caixa de diálogo Configurações secundárias avançadas.

- Cluster

Lista os clusters que estão disponíveis como hosts de proteção secundária. Este campo é obrigatório.

- Máquina virtual de storage (SVM)

Lista os SVMs que estão disponíveis no cluster selecionado. É necessário selecionar um cluster antes da lista SVM ser preenchida. Este campo é obrigatório.

- Agregado

Lista os agregados que estão disponíveis no SVM selecionado. Um cluster deve ser selecionado antes que a lista de agregados seja preenchida. Este campo é obrigatório. A lista de agregados exibe as seguintes informações:

- Classificação

Quando vários agregados satisfazem todos os requisitos de um destino, o rank indica a prioridade na qual o agregado é listado, de acordo com as seguintes condições:

- Um agregado que está localizado em um nó diferente do nó de volume primário é preferível para ativar a separação de domínio de falha.
- É preferível um agregado em um nó com menos volumes para permitir o balanceamento de carga entre nós em um cluster.
- Um agregado que tenha mais espaço livre do que outros agregados é preferido para permitir o balanceamento de capacidade. Uma classificação de 1 significa que o agregado é o mais preferido de acordo com os três critérios.

- Nome agregado

Nome do agregado

- Capacidade disponível
- Quantidade de espaço disponível no agregado para dados
- Pool de recursos

Nome do pool de recursos ao qual o agregado pertence

- Convenção de nomenclatura

Especifica a convenção de nomenclatura padrão aplicada ao volume secundário. Você pode aceitar a convenção de nomenclatura fornecida ou criar uma personalizada. A convenção de nomenclatura pode ter os seguintes atributos: %C, %M, %V e %N, onde %C é o nome do cluster, %M é o nome do SVM, %V é o volume de origem e %N é o nome do nó secundário da topologia.

O campo de convenção de nomenclatura é realçado a vermelho se a sua entrada for inválida. Clicar no link "Nome da visualização" exibe uma visualização da convenção de nomenclatura que você inseriu e o texto de visualização é atualizado dinamicamente à medida que você digita uma convenção de nomenclatura no campo de texto. Se você digitar um valor inválido, as informações inválidas serão exibidas como pontos de interrogação vermelhos na área de visualização. Um sufixo entre 001 e 999 é anexado ao nome secundário quando o relacionamento é criado, substituindo o nnn que é exibido no texto de visualização, com 001 sendo atribuído primeiro, 002 atribuído segundo, e assim por diante.

- **Configurações de relacionamento**

Permite especificar a taxa de transferência máxima, a política SnapVault e a programação SnapVault que a relação de proteção usa:

- Taxa de transferência máxima

Especifica a taxa máxima na qual os dados são transferidos entre clusters pela rede. Se você optar por não usar uma taxa de transferência máxima, a transferência de linha de base entre relacionamentos é ilimitada.

- Política de SnapVault

Especifica a política ONTAP SnapVault para o relacionamento. A predefinição é XDPDefat.

- Criar política

Inicia a caixa de diálogo criar política de SnapVault, que permite criar e usar uma nova política de SnapVault.

- Programação SnapVault

Especifica o agendamento ONTAP SnapVault para o relacionamento. Os horários disponíveis incluem nenhum, 5min, 8hour, diariamente, por hora e semanalmente. O padrão é nenhum, indicando que nenhum agendamento está associado ao relacionamento. Relacionamentos sem agendamentos não têm valores de status de atraso, a menos que pertençam a um serviço de storage.

- Criar Agendamento

Inicia a caixa de diálogo criar Agendamento, que permite criar uma agenda SnapVault.

## Botões de comando

Os botões de comando permitem executar as seguintes tarefas:

- **Cancelar**

Descarta suas seleções e fecha a caixa de diálogo Configurar proteção.

- **Aplicar**

Aplica suas seleções e inicia o processo de proteção.

## Caixa de diálogo criar Agendamento

A caixa de diálogo criar agendamento permite criar um cronograma de proteção básico ou avançado para transferências de relacionamento do SnapMirror e do SnapVault. Você pode criar uma nova programação para aumentar a frequência de transferências de dados devido a atualizações de dados frequentes ou pode criar uma programação menos frequente quando os dados são alterados com pouca frequência.

As programações não podem ser configuradas para relacionamentos síncronos do SnapMirror.

- **Cluster de destino**

O nome do cluster selecionado na guia SnapVault (Configuração) ou SnapMirror (Configuração de proteção) da caixa de diálogo Configurar proteção.

- **Nome da programação**

O nome que você fornece para a programação. Os nomes de programação podem consistir nos caracteres AA Z, a a z, 0 a 9, bem como em qualquer um dos seguintes caracteres especiais: ! \* ( ) \_ -. Os nomes de programação podem não incluir os seguintes caracteres: >.

- **Básico ou Avançado**

O modo de programação que pretende utilizar.

O modo básico inclui os seguintes elementos:

- Repita

Com que frequência ocorre uma transferência agendada. As opções incluem horário, diário e semanal.

- Dia

Quando uma repetição semanal é selecionada, o dia da semana uma transferência ocorre.

- Tempo

Quando Daily (Diário) ou Weekly (semanal) é selecionado, a hora do dia em que ocorre uma transferência.

O modo avançado inclui os seguintes elementos:

- Meses

Uma lista numérica separada por vírgulas que representa os meses do ano. Os valores válidos são de 0 a 11, com zero representando janeiro, e assim por diante. Este elemento é opcional. Deixar o campo em branco implica que as transferências ocorrem todos os meses.

- Dias

Uma lista numérica separada por vírgulas que representa o dia do mês. Os valores válidos são de 1 a 31. Este elemento é opcional. Deixar o campo em branco implica que uma transferência ocorre todos os dias do mês.

- Dias úteis

Uma lista numérica separada por vírgulas que representa os dias da semana. Os valores válidos são de 0 a 6, com 0 representando domingo, e assim por diante. Este elemento é opcional. Deixar o campo em branco implica que uma transferência ocorre todos os dias da semana. Se um dia da semana for especificado, mas um dia do mês não for especificado, uma transferência ocorre apenas no dia especificado da semana e não todos os dias.

- Horas

Uma lista numérica separada por vírgulas que representa o número de horas em um dia. Os valores válidos são de 0 a 23, com 0 representando meia-noite. Este elemento é opcional.

- Minutos

Uma lista numérica separada por vírgulas que representa os minutos em uma hora. Os valores válidos são de 0 a 59. Este elemento é necessário.

## Caixa de diálogo criar política de SnapMirror

A caixa de diálogo criar política de SnapMirror permite criar uma política para definir a prioridade para transferências de SnapMirror. Use políticas para maximizar a eficiência das transferências da origem para o destino.

- **Cluster de destino**

O nome do cluster selecionado na guia SnapMirror da caixa de diálogo Configurar proteção.

- **SVM de destino**

O nome do SVM selecionado na guia SnapMirror da caixa de diálogo Configurar proteção.

- **Nome da política**

O nome fornecido para a nova política. Os nomes de política podem consistir nos caracteres A A Z, a a z, 0 a 9, ponto (.), hífen (-) e sublinhado (\_).

- **Prioridade de transferência**

A prioridade na qual uma transferência é executada para operações assíncronas. Pode selecionar normal ou baixo. Transfira relacionamentos com políticas que especificam uma execução normal de prioridade de transferência antes daqueles com políticas que especificam uma prioridade de transferência baixa.

- **Comentário**

Um campo opcional no qual você pode adicionar comentários sobre a política.

- **\* Reiniciar transferência\***

Indica que ação de reinício deve ser executada quando uma transferência é interrompida por uma operação de cancelamento ou qualquer tipo de falha, como uma interrupção da rede. Pode selecionar uma das seguintes opções:

- Sempre

Especifica que uma nova cópia Snapshot é criada antes de reiniciar uma transferência e, se existir, a transferência é reiniciada a partir de um ponto de verificação, seguida de uma transferência incremental da cópia Snapshot recém-criada.

- Nunca

Especifica que as transferências interrompidas nunca são reiniciadas.

### **Botões de comando**

Os botões de comando permitem executar as seguintes tarefas:

- **Cancelar**

Descarta as seleções e fecha a caixa de diálogo Configurar proteção.

- **Aplicar**

Aplica suas seleções e inicia o processo de proteção.

### **Caixa de diálogo criar política de SnapVault**

A caixa de diálogo criar política de SnapVault permite criar uma política para definir a prioridade para transferências de SnapVault. Você usa políticas para maximizar a eficiência das transferências do volume primário para o secundário.

- **Cluster de destino**

O nome do cluster selecionado na guia SnapVault da caixa de diálogo Configurar proteção.

- **SVM de destino**

O nome do SVM selecionado na guia SnapVault da caixa de diálogo Configurar proteção.

- **Nome da política**

O nome fornecido para a nova política. Os nomes de política podem consistir nos caracteres A A Z, a a z, 0 a 9, ponto (.), hífen (-) e sublinhado (\_).

- **Prioridade de transferência**

A prioridade na qual a transferência é executada. Pode selecionar normal ou baixo. Transfira

relacionamentos com políticas que especificam uma execução normal de prioridade de transferência antes daqueles com políticas que especificam uma prioridade de transferência baixa. A predefinição é normal.

- **Comentário**

Um campo opcional no qual você pode adicionar um comentário de até 255 caracteres sobre a política SnapVault.

- **Ignorar tempo de acesso**

Especifica se as transferências incrementais são ignoradas para arquivos que têm apenas seu tempo de acesso alterado.

- **Etiqueta de replicação**

Lista em uma tabela as regras associadas às cópias Snapshot selecionadas pelo ONTAP que têm um rótulo de replicação específico em uma política. As seguintes informações e ações também estão disponíveis:

- Botões de comando

Os botões de comando permitem executar as seguintes ações:

- Adicionar

Permite criar uma etiqueta de cópia Snapshot e uma contagem de retenção.

- Editar contagem de retenção

Permite alterar a contagem de retenção de uma etiqueta de cópia Snapshot existente. A contagem de retenção deve ser um número entre 1 e 251. A soma de todas as contagens de retenção para todas as regras não pode exceder 251.

- Eliminar

Permite eliminar uma etiqueta de cópia Snapshot existente.

- Etiqueta de cópia Snapshot

Exibe a etiqueta cópia Snapshot. Se você selecionar um ou mais volumes com a mesma política de cópia Snapshot local, uma entrada para cada rótulo na política será exibida. Se você selecionar vários volumes com duas ou mais políticas de cópia Snapshot local, a tabela exibirá todos os rótulos de todas as diretivas

- Programação

Exibe a programação associada a cada etiqueta de cópia Snapshot. Se um rótulo tiver mais de uma programação associada a ele, as programações desse rótulo serão exibidas em uma lista separada por vírgulas. Se você selecionar vários volumes com o mesmo rótulo, mas com horários diferentes, a programação exibirá "vários" para indicar que mais de um agendamento está associado aos volumes selecionados.

- Contagem retenção destino

Exibe o número de cópias Snapshot com o rótulo especificado que são retidas no secundário SnapVault. As contagens de retenção para rótulos com várias programações exibem a soma de



contagens de retenção de cada etiqueta e par de programação. Se você selecionar vários volumes com duas ou mais políticas de cópia Snapshot local, a contagem de retenção estará vazia.

## Caixa de diálogo Editar relação

Você pode editar um relacionamento de proteção existente para alterar a taxa de transferência máxima, a política de proteção ou o cronograma de proteção.

### Informações do destino

- **Cluster de destino**

O nome do cluster de destino selecionado.

- **SVM de destino**

O nome do SVM selecionado

- **Configurações de relacionamento**

Permite especificar a taxa de transferência máxima, a política SnapMirror e a programação que a relação de proteção usa:

- Taxa de transferência máxima

Especifica a taxa máxima na qual os dados de linha de base são transferidos entre clusters pela rede. Quando selecionada, a largura de banda da rede é limitada ao valor especificado. Você pode inserir um valor numérico e selecionar kilobytes por segundo (kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) ou terabytes por segundo (Tbps). A taxa de transferência máxima especificada deve ser superior a 1 kbps e inferior a 4 Tbps. Se você optar por não usar uma taxa de transferência máxima, a transferência de linha de base entre relacionamentos é ilimitada. Se o cluster primário e o cluster secundário forem os mesmos, esta definição é desativada.

- Política de SnapMirror

Especifica a política ONTAP SnapMirror para o relacionamento. A predefinição é DPDefault.

- Criar política

Inicia a caixa de diálogo criar política de SnapMirror, que permite criar e usar uma nova política de SnapMirror.

- Programação SnapMirror

Especifica a política ONTAP SnapMirror para o relacionamento. Os horários disponíveis incluem nenhum, 5min, 8hour, diariamente, por hora e semanalmente. O padrão é nenhum, indicando que nenhum agendamento está associado ao relacionamento. Relacionamentos sem agendamentos não têm valores de status de atraso, a menos que pertençam a um serviço de storage.

- Criar Agendamento

Inicia a caixa de diálogo criar Agendamento, que permite criar uma nova agenda SnapMirror.

## Botões de comando

Os botões de comando permitem executar as seguintes tarefas:

- **Cancelar**

Descarta as seleções e fecha a caixa de diálogo Configurar proteção.

- **Submeter**

Aplica suas seleções e fecha a caixa de diálogo Editar relacionamento.

## Caixa de diálogo Inicializar/Atualizar

A caixa de diálogo Inicializar/Atualizar permite que você execute uma transferência de linha de base pela primeira vez em um novo relacionamento de proteção ou atualize um relacionamento se ele já estiver inicializado e você quiser executar uma atualização incremental manual, não programada.

### Guia Opções de transferência

A guia Opções de transferência permite alterar a prioridade de inicialização de uma transferência e alterar a largura de banda usada durante as transferências.

- **Prioridade de transferência**

A prioridade na qual a transferência é executada. Pode selecionar normal ou baixo. Relacionamentos com políticas que especificam uma execução normal de prioridade de transferência antes daquelas que especificam uma prioridade de transferência baixa. Normal é selecionado por padrão.

- **Taxa de transferência máxima**

Especifica a taxa máxima na qual os dados são transferidos entre clusters pela rede. Se você optar por não usar uma taxa de transferência máxima, a transferência de linha de base entre relacionamentos é ilimitada. Se selecionar mais de uma relação com diferentes taxas de transferência máximas, pode especificar uma das seguintes definições de taxa de transferência máxima:

- Use valores especificados durante a configuração ou edição de relacionamento individual

Quando selecionadas, as operações de inicialização e atualização usam a taxa de transferência máxima especificada no momento da criação ou edição de cada relacionamento. Este campo só está disponível quando várias relações com diferentes taxas de transferência estão sendo inicializadas ou atualizadas.

- Ilimitado

Indica que não há limitação de largura de banda nas transferências entre relacionamentos. Este campo só está disponível quando várias relações com diferentes taxas de transferência estão sendo inicializadas ou atualizadas.

- Limite a largura de banda para

Quando selecionada, a largura de banda da rede é limitada ao valor especificado. Você pode inserir um valor numérico e selecionar kilobytes por segundo (kbps), megabytes por segundo (Mbps),

Gigabytes por segundo (Gbps) ou Terabytes por segundo (Tbps). A taxa de transferência máxima especificada deve ser superior a 1 kbps e inferior a 4 Tbps.

### Guia cópias Snapshot de origem

A guia cópias Snapshot de origem exibe as seguintes informações sobre a cópia Snapshot de origem usada para a transferência da linha de base:

- **Volume da fonte**

Exibe os nomes dos volumes de origem correspondentes.

- **Volume de destino**

Apresenta os nomes dos volumes de destino selecionados.

- **Tipo de fonte**

Apresenta o tipo de volume. O tipo pode ser leitura/escrita ou proteção de dados.

- **Cópia Snapshot**

Exibe a cópia Snapshot usada para a transferência de dados. Clicar no valor cópia Instantânea exibe a caixa de diálogo Selecionar cópia Instantânea de origem, na qual você pode selecionar uma cópia Snapshot específica para sua transferência, dependendo do tipo de relação de proteção que você tem e da operação que está executando. A opção de especificar uma cópia Snapshot diferente não está disponível para fontes de tipo de proteção de dados.

### Botões de comando

Os botões de comando permitem executar as seguintes tarefas:

- **Cancelar**

Descarta suas seleções e fecha a caixa de diálogo Inicializar/Atualizar.

- **Submeter**

Guarda as suas seleções e inicia o trabalho de inicialização ou atualização.

### Ressincronizar a caixa de diálogo

A caixa de diálogo Resincronizar permite que você sincronize novamente os dados em um relacionamento SnapMirror ou SnapVault que foi quebrado anteriormente e, em seguida, o destino foi feito um volume de leitura/gravação. Você também pode ressincronizar quando uma cópia Snapshot comum necessária no volume de origem for excluída, causando falha nas atualizações do SnapMirror ou do SnapVault.

### Guia Opções de ressincronização

A guia Opções de ressincronização permite definir a prioridade de transferência e a taxa máxima de transferência para a relação de proteção que você está ressincronizando.

- **Prioridade de transferência**

A prioridade na qual a transferência é executada. Pode selecionar normal ou baixo. Relacionamentos com políticas que especificam uma prioridade de transferência normal são executados antes daqueles com políticas que especificam uma prioridade de transferência baixa.

- **Taxa de transferência máxima**

Especifica a taxa máxima na qual os dados são transferidos entre clusters pela rede. Quando selecionada, a largura de banda da rede é limitada ao valor especificado. Você pode inserir um valor numérico e selecionar kilobytes por segundo (kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) ou Tbps. Se você optar por não usar uma taxa de transferência máxima, a transferência de linha de base entre relacionamentos é ilimitada.

### **Guia cópias Snapshot de origem**

A guia cópias Snapshot de origem exibe as seguintes informações sobre a cópia Snapshot de origem usada para a transferência da linha de base:

- **Volume da fonte**

Exibe os nomes dos volumes de origem correspondentes.

- **Volume de destino**

Apresenta os nomes dos volumes de destino selecionados.

- **Tipo de fonte**

Exibe o tipo de volume: Leitura/gravação ou proteção de dados.

- **Cópia Snapshot**

Exibe a cópia Snapshot usada para a transferência de dados. Clicar no valor cópia Instantânea exibe a caixa de diálogo Selecionar cópia Instantânea de origem, na qual pode selecionar uma cópia Snapshot específica para sua transferência, dependendo do tipo de relação de proteção que você tem e da operação que está executando.

### **Botões de comando**

- **Submeter**

Inicia o processo de resincronização e fecha a caixa de diálogo Resincronizar.

- **Cancelar**

Cancela suas seleções e fecha a caixa de diálogo Resincronizar.

### **Selecione a caixa de diálogo cópia Instantânea de origem**

Use a caixa de diálogo Selecionar cópia Snapshot de origem para selecionar uma cópia Snapshot específica para transferir dados entre relacionamentos de proteção ou selecione o comportamento padrão, que varia dependendo se você está inicializando,

atualizando ou ressincronizando um relacionamento e se o relacionamento é um SnapMirror ou SnapVault.

#### Padrão

Permite selecionar o comportamento padrão para determinar qual cópia Snapshot é usada para inicializar, atualizar e ressincronizar transferências para relacionamentos SnapVault e SnapMirror.

Se você estiver executando uma transferência SnapVault, o comportamento padrão para cada operação é o seguinte:

<b>Operação</b>	<b>Comportamento padrão do SnapVault quando a fonte é leitura/gravação</b>	<b>Comportamento padrão do SnapVault quando a origem é proteção de dados (DP)</b>
Inicializar	Cria uma nova cópia Snapshot e a transfere.	Transfere a última cópia Snapshot exportada.
Atualização	Transfere apenas cópias Snapshot rotuladas, conforme especificado na política.	Transfere a última cópia Snapshot exportada.
Ressincronizar	Transfere todas as cópias Snapshot identificadas criadas após a cópia Snapshot comum mais recente.	Transfere a mais recente cópia Snapshot rotulada.

Se você estiver executando uma transferência SnapMirror, o comportamento padrão para cada operação é o seguinte:

<b>Operação</b>	<b>Comportamento padrão do SnapMirror</b>	<b>Comportamento padrão do SnapMirror quando o relacionamento é segundo salto em uma cascata SnapMirror to SnapMirror</b>
Inicializar	Cria uma nova cópia Snapshot e transfere-a para todas as cópias Snapshot criadas antes da nova cópia Snapshot.	Transfere todas as cópias Snapshot da origem.
Atualização	Cria uma nova cópia Snapshot e transfere-a para todas as cópias Snapshot criadas antes da nova cópia Snapshot.	Transfere todas as cópias Snapshot.

<b>Operação</b>	<b>Comportamento padrão do SnapMirror</b>	<b>Comportamento padrão do SnapMirror quando o relacionamento é segundo salto em uma cascata SnapMirror to SnapMirror</b>
Ressincronizar	Cria uma nova cópia Snapshot e transfere todas as cópias Snapshot da origem.	Transfere todas as cópias Snapshot do volume secundário para o volume terciário, e exclui todos os dados adicionados após a criação da cópia Snapshot comum mais recente.

### **Cópia Snapshot existente**

Permite selecionar uma cópia Snapshot existente na lista se a seleção de cópia Snapshot for permitida para essa operação.

- **Cópia Snapshot**

Exibe as cópias Snapshot existentes a partir das quais você pode selecionar para uma transferência.

- **Data de criação**

Exibe a data e a hora em que a cópia Snapshot foi criada. As cópias snapshot são listadas das mais recentes às menos recentes, sendo as mais recentes no topo da lista.

Se você estiver executando uma transferência SnapVault e quiser selecionar uma cópia Snapshot existente para transferir de uma origem para um destino, o comportamento de cada operação será o seguinte:

<b>Operação</b>	<b>Comportamento do SnapVault ao especificar uma cópia Snapshot</b>	<b>Comportamento do SnapVault ao especificar uma cópia Snapshot em uma cascata</b>
Inicializar	Transfere a cópia Snapshot especificada.	A seleção de cópia Snapshot de origem não é compatível com volumes de proteção de dados.
Atualização	Transfere a cópia Snapshot especificada.	A seleção de cópia Snapshot de origem não é compatível com volumes de proteção de dados.
Ressincronizar	Transfere a cópia Snapshot selecionada.	A seleção de cópia Snapshot de origem não é compatível com volumes de proteção de dados.

Se você estiver executando uma transferência SnapMirror e quiser selecionar uma cópia Snapshot existente para transferir de uma origem para um destino, o comportamento de cada operação será o seguinte:

<b>Operação</b>	<b>Comportamento do SnapMirror ao especificar uma cópia Snapshot</b>	<b>Comportamento do SnapMirror ao especificar uma cópia Snapshot em uma cascata</b>
Inicializar	Transfere todas as cópias Snapshot na origem, até a cópia Snapshot especificada.	A seleção de cópia Snapshot de origem não é compatível com volumes de proteção de dados.
Atualização	Transfere todas as cópias Snapshot na origem, até a cópia Snapshot especificada.	A seleção de cópia Snapshot de origem não é compatível com volumes de proteção de dados.
Ressincronizar	Transfere todas as cópias snapshot da origem, até a cópia Snapshot selecionada e, em seguida, exclui todos os dados adicionados após a criação da cópia Snapshot comum mais recente.	A seleção de cópia Snapshot de origem não é compatível com volumes de proteção de dados.

#### **Botões de comando**

Os botões de comando permitem executar as seguintes tarefas:

- **Submeter**

Envia suas seleções e fecha a caixa de diálogo Selecionar cópia Snapshot de origem.

- **Cancelar**

Descarta suas seleções e fecha a caixa de diálogo Selecionar cópia Instantânea de origem.

#### **Caixa de diálogo Reverter Resync**

Quando você tem uma relação de proteção que é quebrada porque o volume de origem está desativado e o destino é feito um volume de leitura/gravação, a ressincronização reversa permite reverter a direção da relação para que o destino se torne a nova fonte e a origem se torne o novo destino.

Quando um desastre desativa o volume de origem em sua relação de proteção, você pode usar o volume de destino para servir dados convertendo-os para leitura/gravação, enquanto você repara ou substituir a fonte, atualizar a fonte e restabelecer a relação. Quando você executa uma operação de ressincronização reversa, os dados na fonte mais recente do que os dados na cópia Snapshot comum são excluídos.

#### **Antes da ressincronização inversa**

Exibe a origem e o destino de uma relação antes de uma operação de ressincronização reversa.

- **Volume da fonte**

O nome e a localização do volume de origem antes de uma operação de ressincronização reversa.

- **Volume de destino**

O nome e a localização do volume de destino antes de uma operação de resincronização reversa.

#### Após a resincronização inversa

Exibe qual é a origem e o destino de uma relação após uma operação de resincronização de reserva.

- **Volume da fonte**

O nome e a localização do volume de origem após uma operação de resincronização reversa.

- **Volume de destino**

O nome e a localização do volume de destino após uma operação de resincronização reversa.

#### Botões de comando

Os botões de comando permitem executar as seguintes ações:

- **Submeter**

Inicia o processo de resincronização reversa.

- **Cancelar**

Fecha a caixa de diálogo Reverse Resync sem iniciar uma operação de resincronização reversa.

#### Relacionamento: Todos os relacionamentos são exibidos

A exibição relação: Todas as relações exibe informações sobre relacionamentos de proteção no sistema de armazenamento.

Por padrão, quando você acessa a página relacionamentos, o relatório exibido inclui as relações de proteção de nível superior para volumes e VMs de armazenamento. Os controles ao longo da parte superior da página permitem selecionar uma exibição específica, realizar pesquisas para localizar objetos específicos, criar e aplicar filtros para restringir a lista de dados exibidos, adicionar/remover/reordenar colunas na página e exportar os dados na página para um arquivo .csv, .pdf ou .xlsx. Depois de personalizar a página, você pode salvar os resultados como uma visualização personalizada e, em seguida, agendar um relatório desses dados para ser gerado e enviado por e-mail regularmente. Por padrão, quando você seleciona o menu **relacionamentos**, o relatório exibido inclui relações de proteção para volumes e VMs de armazenamento em seu datacenter. Você pode usar a opção **Filter** para visualizar apenas sistemas de armazenamento selecionados, como apenas volumes ou apenas VMs de armazenamento. O mesmo relatório é exibido na página armazenamento e somente para a entidade de armazenamento selecionada. Se você quiser ver as relações de VM de volume ou armazenamento, você pode acessar a página **Storage > volumes > relacionamento: Todos os relacionamentos** ou acessar **proteção > relacionamentos > relacionamento: Todos os relacionamentos** e usar a opção **tipo de objeto de relacionamento** no **filtro** para filtrar apenas volumes ou dados de VMs de armazenamento.

A página relacionamentos que lista todas as relações de proteção tem o link **Exibir no Gerenciador do sistema** para o cluster de destino que permite exibir os mesmos objetos no Gerenciador do sistema do ONTAP.



- **Status**

Exibe o status atual da relação de proteção.

O status pode ser um erro (❗), Aviso (⚠) ou OK (✅).

- **Armazenamento de origem VM**

Exibe o nome da SVM de origem. Para ver mais detalhes sobre a fonte SVM, clique no nome do SVM.

Quando um SVM existe no cluster, mas ainda não foi adicionado ao inventário do Unified Manager, ou se o SVM foi criado após a última atualização do cluster, esse campo ficará vazio. Você deve garantir que o SVM exista ou realizar um reconhecimento no cluster para atualizar a lista de recursos.

- **Fonte**

Exibe o volume de origem ou a VM de armazenamento de origem protegida com base na sua seleção. Para ver mais detalhes sobre o volume de origem ou a VM de armazenamento, clique no nome da VM de volume ou armazenamento.

Se a mensagem `Resource-key not discovered` for exibida, isso poderá indicar que o volume existe no cluster, mas ainda não foi adicionado ao inventário do Unified Manager, ou que o volume foi criado após a última atualização do cluster. Você deve garantir que o volume existe ou realizar uma redescoberta no cluster para atualizar a lista de recursos.

- **Armazenamento de destino VM**

Exibe o nome do SVM de destino. Para ver mais detalhes sobre o SVM de destino, clique no nome do SVM.

- **Destino**

Exibe o nome do volume de destino ou da VM de armazenamento com base na sua seleção. Você pode ver mais detalhes sobre o volume de destino ou a VM de armazenamento clicando no respectivo nome do objeto.

- **Tipo Objeto relação**

Exibe o tipo de objeto usado na relação, como VM de armazenamento, volume e Grupo de consistência. Para objetos em um relacionamento de consistência, a origem e os destinos do relacionamento exibem o Grupo de consistência e, clicando neles, você acessa a página LUNs para exibir o relacionamento.

- **Política**

Exibe o nome da política de proteção para o relacionamento SnapMirror. Você pode clicar no nome da política para exibir detalhes associados a essa política, incluindo as seguintes informações:

- Prioridade de transferência

Especifica a prioridade na qual uma transferência é executada para operações assíncronas. A prioridade de transferência é normal ou baixa. As transferências prioritárias normais são agendadas antes das transferências de baixa prioridade. O padrão é normal.

- Ignore o tempo de acesso

Aplica-se apenas às relações SnapVault. Isso especifica se as transferências incrementais ignoram

arquivos que têm apenas seu tempo de acesso alterado. Os valores são verdadeiro ou Falso. O padrão é Falso.

- Quando a relação está fora de sincronia

Especifica a ação que o ONTAP executa quando um relacionamento síncrono não é capaz de ser sincronizado. As relações StrictSync restringirão o acesso ao volume primário se houver uma falha na sincronização com o volume secundário. As relações de sincronização não restringem o acesso ao primário se houver uma falha na sincronização com o secundário.

- Limite de tentativas

Especifica o número máximo de vezes para tentar cada transferência manual ou programada para um relacionamento SnapMirror. A predefinição é 8.

- Comentários

Fornece um campo de texto para comentários específicos para a política selecionada.

- Etiqueta SnapMirror

Especifica o rótulo SnapMirror para a primeira programação associada à política de cópia Snapshot. O rótulo SnapMirror é usado pelo subsistema SnapVault quando você faz backup de cópias snapshot em um destino SnapVault.

- Definição de retenção

Especifica por quanto tempo os backups são mantidos, com base no tempo ou no número de backups.

- Cópias Snapshot reais

Especifica o número de cópias Snapshot nesse volume que corresponde ao rótulo especificado.

- Preservar cópias Snapshot

Especifica o número de cópias Snapshot do SnapVault que não são excluídas automaticamente, mesmo que o limite máximo da política seja atingido. Os valores são verdadeiro ou Falso. O padrão é Falso.

- Limite de aviso de retenção

Especifica o limite de cópia Snapshot no qual um aviso é enviado para indicar que o limite máximo de retenção está quase atingido.

- **Duração do atraso**

Exibe o tempo que os dados no espelho ficam atrás da fonte.

A duração do atraso deve ser próxima ou igual a 0 segundos para relacionamentos StrictSync.

- **Estado de lag**

Exibe o status de atraso para relacionamentos gerenciados e para relacionamentos não gerenciados que têm uma programação associada a esse relacionamento. O estado de atraso pode ser:

- Erro

A duração do atraso é maior ou igual ao limite de erro de atraso.

- Aviso

A duração do atraso é superior ou igual ao limite de aviso de atraso.

- OK

A duração do atraso está dentro dos limites normais.

- Não aplicável

O status de atraso não é aplicável a relacionamentos síncronos porque uma programação não pode ser configurada.

- \* Última atualização bem-sucedida \*

Apresenta a hora da última operação de SnapMirror ou SnapVault bem-sucedida.

A última atualização bem-sucedida não se aplica a relacionamentos síncronos.

- \* Relacionamentos constitutivos\*

Exibe se existem volumes no objeto selecionado.

- **Tipo de relacionamento**

Exibe o tipo de relação usado para replicar um volume. Os tipos de relacionamento incluem:

- Espelhamento assíncrono
- Cofre assíncrono
- MirrorVault assíncrono
- StrictSync
- Sincronizar

- **Status da transferência**

Exibe o status da transferência para a relação de proteção. O estado da transferência pode ser um dos seguintes:

- A abortar

As transferências SnapMirror estão ativadas; no entanto, uma operação de cancelamento de transferência que pode incluir a remoção do ponto de verificação está em andamento.

- Verificação

O volume de destino está passando por uma verificação de diagnóstico e nenhuma transferência está em andamento.

- A finalizar

As transferências SnapMirror estão ativadas. O volume está atualmente na fase pós-transferência para transferências incrementais de SnapVault.

- Ocioso

As transferências estão ativadas e nenhuma transferência está em curso.

- Sincronização in-Sync

Os dados nos dois volumes na relação síncrona são sincronizados.

- Fora de sincronização

Os dados no volume de destino não são sincronizados com o volume de origem.

- Preparar

As transferências SnapMirror estão ativadas. O volume está atualmente na fase de pré-transferência para transferências incrementais de SnapVault.

- Em fila de espera

As transferências SnapMirror estão ativadas. Nenhuma transferência está em andamento.

- Quiesced

As transferências SnapMirror estão desativadas. Nenhuma transferência está em andamento.

- Quiescing

Uma transferência SnapMirror está em andamento. As transferências adicionais estão desativadas.

- A transferir

As transferências SnapMirror estão ativadas e uma transferência está em curso.

- Em transição

A transferência assíncrona de dados da origem para o volume de destino está concluída e a transição para a operação síncrona foi iniciada.

- A aguardar

Uma transferência SnapMirror foi iniciada, mas algumas tarefas associadas estão aguardando para serem enfileiradas.

- **Duração da última transferência**

Apresenta o tempo necessário para a última transferência de dados ser concluída.

A duração da transferência não é aplicável às relações StrictSync porque a transferência deve ser simultânea.

- \* Último tamanho de transferência \*

Exibe o tamanho, em bytes, da última transferência de dados.

O tamanho da transferência não se aplica às relações StrictSync.

- **Mediadores**

Exibe o status do mediador.

- Não aplicável

Se o cluster não suportar a sincronização ativa do SnapMirror.

- Não configurado

Se não estiver configurado ou se estiver configurado, mas apenas o cluster de destino for adicionado e o cluster de origem não for adicionado ao Unified Manager.

- Endereço IP do mediador

Se estiver configurado, e os clusters de origem e destino serão adicionados ao Unified Manager.

- **Estado**

Exibe o estado da relação SnapMirror ou SnapVault. O estado pode ser não inicializado, SnapMirrored ou quebrado. Se for selecionado um volume de origem, o estado da relação não é aplicável e não é apresentado.

- **Saúde do relacionamento**

Exibe a faixa de relacionamento do cluster.

- \* Motivo não saudável\*

A razão pela qual o relacionamento está em um estado insalubre.

- **Prioridade de transferência**

Exibe a prioridade na qual uma transferência é executada. A prioridade de transferência é normal ou baixa. As transferências prioritárias normais são agendadas antes das transferências de baixa prioridade.

A prioridade de transferência não se aplica a relacionamentos síncronos porque todas as transferências são tratadas com a mesma prioridade.

- **Programação**

Exibe o nome da programação de proteção atribuída à relação.

A programação não é aplicável para relacionamentos síncronos.

- **Versão replicação flexível**

Exibe Sim, Sim com a opção de backup ou nenhum.

- **Cluster de origem**

Exibe o FQDN, o nome curto ou o endereço IP do cluster de origem para a relação SnapMirror.

- **FQDN do cluster de origem**

Exibe o nome do cluster de origem para a relação SnapMirror.

- **Nó de origem**

Exibe o nome do link de nome do nó de origem para a relação SnapMirror de um volume e exibe o link de contagem de nós de relacionamento SnapMirror quando o objeto é uma VM de armazenamento ou Grupo de consistência.

Na exibição personalizada, quando você clica no link do nome do nó, você pode exibir e estender a proteção para objetos de storage nos quais os volumes desses grupos de consistência pertencem a uma relação de sincronização ativa do SnapMirror.

Quando você clica no link de contagem de nós, ele o leva para a página de nó com os respectivos nós associados a essa relação. Quando a contagem de nós é 0, não há nenhum valor exibido, pois não há nós associados à relação.

- **Nó de destino**

Exibe o nome do link de nome do nó de destino para a relação SnapMirror de um volume e exibe o link de contagem de nós de relacionamento SnapMirror quando o objeto é uma VM de armazenamento ou Grupo de consistência.

Quando você clica no link de contagem de nós, ele o leva para a página de nó com os respectivos nós associados a essa relação. Quando a contagem de nós é 0, não há nenhum valor exibido, pois não há nós associados à relação.

- **Cluster de destino**

Exibe o nome do cluster de destino para a relação SnapMirror.

- **FQDN** do cluster de destino

Exibe o FQDN, o nome curto ou o endereço IP do cluster de destino para a relação SnapMirror.

- **Protegido por**

Exibe as diferentes relações. Nessa coluna, é possível exibir relacionamentos de grupo de volume e consistência para clusters e pedidos de máquinas virtuais de armazenamento, incluindo:

- SnapMirror
- Storage VM DR
- SnapMirror, Storage VM DR
- Grupo de consistência
- SnapMirror, Grupo de consistência.

## Informações relacionadas

- Para obter informações sobre a visualização **relacionamento: MetroCluster**, "[Monitoramento de configurações do MetroCluster](#)" consulte .
- Para obter informações sobre a 1 visualização **relação: Status de transferência do último mês**, "[Relação: Último 1 mês visualização do Status da transferência](#)" consulte .
- Para obter informações sobre a visualização **relacionamento: Todas as relações**, "[Relação: Último 1 mês visualização da taxa de transferência](#)" consulte .

## Relação: Último 1 mês visualização do Status da transferência

O modo de exibição relacionamento: Último status de transferência de 1 meses permite analisar as tendências de transferência ao longo de um período de tempo para volumes e VMs de armazenamento em relacionamentos assíncronos. Esta página também mostra se a transferência foi um sucesso ou uma falha.

Os controles ao longo da parte superior da página permitem que você execute pesquisas para localizar objetos específicos, criar e aplicar filtros para restringir a lista de dados exibidos, adicionar/remover/reordenar colunas na página e exportar os dados na página para um `.csv` arquivo, ou `.xlsx` ou `.pdf`. Depois de personalizar a página, você pode salvar os resultados como uma visualização personalizada e, em seguida, agendar um relatório desses dados para ser gerado e enviado por e-mail regularmente. Você pode usar a opção **filtro** para exibir somente sistemas de armazenamento selecionados, como somente volumes ou somente VMs de armazenamento. O mesmo relatório é exibido na página armazenamento e somente para a entidade de armazenamento selecionada. Por exemplo, se você quiser ver as relações de volume, você pode acessar o relatório de status de transferência dos últimos 1 meses para as VMs de armazenamento a partir do menu **armazenamento > VMs de armazenamento > relação: Último 1 mês Status de transferência** ou do menu **proteção > relacionamentos > relação: Último 1 mês Status de transferência** e usar o **filtro** para visualizar somente os dados para volumes.

- **Volume da fonte**

Exibe o nome do volume de origem.

- **Volume de destino**

Apresenta o nome do volume de destino.

- **Tipo de operação**

Apresenta o tipo de transferência de volume.

- **Resultado da operação**

Apresenta se a transferência de volume foi bem-sucedida.

- **Hora de início da transferência**

Apresenta a hora de início da transferência de volume.

- \* Tempo de término da transferência\*

Apresenta a hora de fim da transferência de volume.

- **Duração da transferência**

Apresenta o tempo necessário (em horas) para concluir a transferência de volume.

- \* Tamanho da transferência\*

Exibe o tamanho (em MB) do volume transferido.

- **Fonte SVM**

Exibe o nome da máquina virtual de storage (SVM).

- **Cluster de origem**

Exibe o nome do cluster de origem.

- **SVM de destino**

Exibe o nome do SVM de destino.

- **Cluster de destino**

Exibe o nome do cluster de destino.

## Informações relacionadas

- Para obter informações sobre a visualização **relacionamento: Todas as relações**, "[Relacionamento: Todos os relacionamentos são exibidos](#)" consulte .
- Para obter informações sobre a visualização **relação:MetroCluster**, "[Monitoramento de configurações do MetroCluster](#)" consulte .
- Para obter informações sobre a visualização **relacionamento: Todas as relações**, "[Relação: Último 1 mês visualização da taxa de transferência](#)" consulte .

## Relação: Último 1 mês visualização da taxa de transferência

O modo de exibição relação: Taxa de transferência de 1 meses último permite analisar a quantidade de volume de dados que é transferido diariamente para volumes em relacionamentos assíncronos. Esta página também fornece detalhes sobre transferências diárias e o tempo necessário para concluir a operação de transferência de volumes e VMs de armazenamento.

Os controles ao longo da parte superior da página permitem que você execute pesquisas para localizar objetos específicos, criar e aplicar filtros para restringir a lista de dados exibidos, adicionar/remover/reordenar colunas na página e exportar os dados na página para um arquivo .csv, .pdf ou .xlsx. Depois de personalizar a página, você pode salvar os resultados como uma visualização personalizada e, em seguida, agendar um relatório desses dados para ser gerado e enviado por e-mail regularmente. Por exemplo, se você quiser ver relacionamentos de volume, você pode acessar o menu **Storage > volumes > relacionamento: Último 1 mês taxa de transferência** ou acessar **proteção > relacionamentos > relacionamentos:último 1 mês taxa de transferência\*** e usar o **filtro** para exibir somente os dados para volumes.

- \* Tamanho total da transferência\*

Exibe o tamanho total da transferência de volume em gigabytes.

- **Dia**

Apresenta o dia em que a transferência de volume foi iniciada.

- **Hora de fim**

Exibe a hora de término da transferência de volume com a data.

## Informações relacionadas



- Para obter informações sobre a visualização **relação:MetroCluster**, "[Monitoramento de configurações do MetroCluster](#)" consulte .
- Para obter informações sobre a 1 visualização **relação: Status de transferência do último mês**, "[Relação: Último 1 mês visualização do Status da transferência](#)" consulte .
- Para obter informações sobre a visualização **relacionamento: Todas as relações**, consulte "[Relação: Último 1 mês visualização da taxa de transferência](#)"

# Gerar relatórios personalizados

## Relatórios do Unified Manager

O Active IQ Unified Manager (anteriormente conhecido como Gerenciador Unificado de OnCommand) permite visualizar, personalizar, baixar e agendar relatórios para seus sistemas de storage da ONTAP. Os relatórios podem fornecer detalhes sobre a capacidade, a integridade, a performance, a segurança e as relações de proteção do sistema de storage.

O novo recurso de agendamento e geração de relatórios do Unified Manager introduzido no Active IQ Unified Manager 9,6 substitui o mecanismo de relatórios anterior que foi desativado no Unified Manager versão 9,5.

Os relatórios fornecem diferentes visualizações de sua rede, oferecendo informações úteis sobre capacidade, integridade, desempenho, segurança e dados de proteção. Você pode personalizar suas visualizações mostrando, ocultando e reorganizando colunas, filtrando dados, classificando dados e pesquisando os resultados. Você pode salvar exibições personalizadas para reutilização, baixá-las como relatórios e agendá-las como relatórios recorrentes para distribuir por e-mail.

Você pode baixar visualizações no formato Microsoft Excel e personalizá-las. Você pode usar recursos avançados do Excel, como sortes complexos, filtros em camadas, tabelas dinâmicas e gráficos. Quando estiver satisfeito com o relatório do Excel resultante, você pode fazer o upload do arquivo do Excel para uso sempre que o relatório for agendado e compartilhado.

Além de gerar relatórios a partir da interface do usuário, você pode extrair dados de integridade, segurança e desempenho do Unified Manager usando esses métodos adicionais:

- Usando as ferramentas ODBC (Open Database Connectivity) e ODBC para acessar diretamente o banco de dados para obter informações de cluster
- Executando as APIs REST do Unified Manager para retornar as informações que você está interessado em analisar

A partir desta versão do Active IQ Unified Manager, as seguintes melhorias são feitas nos relatórios:

- O e-mail é enviado para um relatório de acordo com a programação configurada. Mesmo quando você gera um relatório sob demanda, você receberá um e-mail.
- O nome do arquivo do relatório e os metadados do relatório incluem o nome do host de onde o relatório foi gerado. Mesmo que alguém altere o nome do arquivo, ainda assim você pode identificar o nome do host de onde o relatório foi gerado devido a esse aprimoramento.

## Pontos de acesso para geração de relatórios

Você pode coletar informações no Unified Manager sobre seus clusters para criar relatórios a partir da IU, consultas de banco de dados MySQL e APIs REST.

Essas seções descrevem os relatórios e o agendamento do Unified Manager por meio da IU.

Há três maneiras de acessar as funcionalidades de relatórios fornecidas pelo Unified Manager:

- Extraindo dados diretamente das páginas de inventário na IU.

- Usando as ferramentas ODBC (Open Database Connectivity) e ODBC para acessar todos os objetos disponíveis.
- Executando as APIs REST do Unified Manager para retornar as informações que você deseja revisar.

Essas seções descrevem os relatórios e o agendamento do Unified Manager por meio da IU.

### Bancos de dados do Unified Manager acessíveis para relatórios personalizados

O Unified Manager usa um banco de dados MySQL para armazenar dados dos clusters que ele está monitorando. Os dados são persistidos em vários esquemas no banco de dados MySQL.

Todos os dados de tabela dos seguintes bancos de dados estão disponíveis:

Banco de dados	Descrição
NetApp_model	Dados sobre os objetos nos controladores ONTAP.
NetApp_model_view	Dados sobre os objetos em controladores ONTAP, adequados para o consumo de ferramentas de relatório.
NetApp_performance	Contadores de desempenho específicos de cluster.
ocum	Dados e informações do aplicativo Unified Manager para oferecer suporte à filtragem, classificação e cálculo de alguns campos derivados da interface do usuário.
ocum_report	Dados para configuração de inventário e informações relacionadas à capacidade.
ocum_report_birt	Visualizações para configuração de inventário e dados relacionados à capacidade, adequadas para consumo de ferramentas de relatório.
opm	Configurações de desempenho e informações de limite.
scalemonitor	Dados sobre problemas de integridade e performance da aplicação do Unified Manager.
vmware_model	Dados de objeto VMware para datastores hospedados no storage NetApp.
vmware_model_view	Visualizações para dados de objetos VMware para datastores hospedados no storage NetApp, adequadas para o consumo de ferramentas de relatório.

Banco de dados	Descrição
vmware_performance	Dados de contador de desempenho da VMware para datastores hospedados no storage NetApp.

Um usuário de relatório — um usuário de banco de dados com a função Report Schema — é capaz de acessar os dados nessas tabelas. Esse usuário tem acesso somente leitura a relatórios e outras visualizações de banco de dados diretamente do banco de dados do Unified Manager. Observe que esse usuário não tem permissão para acessar nenhuma tabela que contenha dados de usuário ou informações de credenciais de cluster.

### APIs REST do Unified Manager que podem ser usadas para geração de relatórios

Você pode usar as APIs REST para ajudar a gerenciar clusters visualizando as informações de integridade, capacidade, desempenho e segurança capturadas pelo Unified Manager.

As APIs REST são expostas por meio da página da Web do Swagger. Você pode acessar a página da Web do Swagger para exibir a documentação da API REST do Unified Manager, bem como emitir manualmente uma chamada de API. Na IU da Web do Unified Manager, na barra de menus, clique no botão **Ajuda** e selecione **Documentação da API**. Para obter informações sobre as APIs REST do Unified Manager, "[Primeiros passos com as APIs REST do Active IQ Unified Manager](#)" consulte .

Você deve ter a função Operador, Administrador de armazenamento ou Administrador de aplicativo para acessar as APIs REST.

### Entendendo relatórios

Os relatórios exibem informações detalhadas sobre armazenamento, rede, qualidade de serviço e relacionamentos de proteção, ajudando você a identificar e resolver possíveis problemas antes que eles ocorram.

Quando você personaliza uma exibição, você pode salvá-la com um nome exclusivo para uso futuro. Você pode agendar um relatório com base nessa visualização para ser executado regularmente e compartilhá-lo com outras pessoas. Você também pode baixar a exibição no Excel para personalizá-la usando recursos avançados do Excel e, em seguida, fazer o upload desse arquivo de volta para o Unified Manager . Se você agendar um relatório usando essa exibição, ele usará o arquivo do Excel que você enviou para criar relatórios robustos que você pode compartilhar.

Você pode gerenciar todos os relatórios que foram agendados na página Agenda de relatórios.



Você deve ter a função Administrador de aplicativos ou Administrador de armazenamento para gerenciar relatórios.

Você pode fazer o download de relatórios como valores separados por vírgulas (CSV), Excel ou arquivos PDF.

### Compreender a relação de visualização e relatório

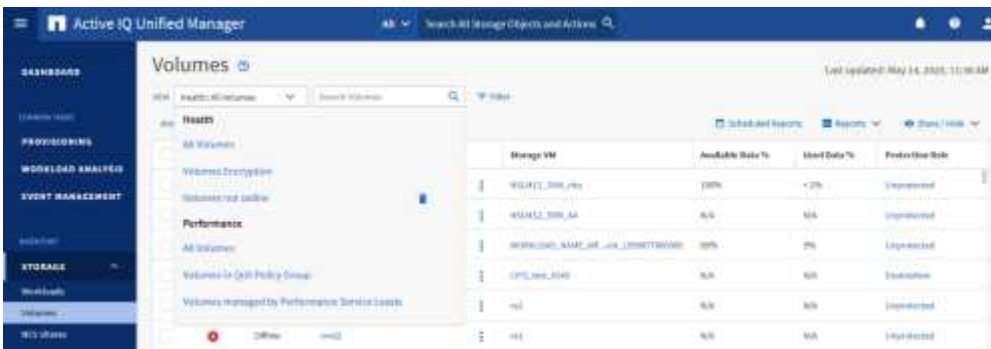
Visualizações e páginas de inventário tornam-se relatórios quando você baixa ou os agenda.

Você pode personalizar e salvar visualizações e páginas de inventário para reutilização. Quase tudo o que você pode visualizar no Unified Manager pode ser salvo, reutilizado, personalizado, agendado e compartilhado como um relatório.

Na lista suspensa Exibir, os itens com o ícone excluir são exibições personalizadas existentes que você ou outro usuário criou. Itens sem um ícone são exibições padrão fornecidas com o Unified Manager. As vistas predefinidas não podem ser modificadas ou eliminadas.



- Se você excluir uma exibição personalizada da lista, ela também excluirá os arquivos do Excel ou os relatórios programados que usam essa exibição.
- Se você alterar uma exibição personalizada, os relatórios que usam essa exibição refletirão a alteração na próxima vez que o relatório for gerado e enviado por e-mail de acordo com a programação do relatório. Ao alterar exibições, verifique se as alterações funcionam com qualquer personalização associada do Excel usada para os relatórios. Se necessário, você pode atualizar o arquivo do Excel baixando-o, fazendo as alterações necessárias e carregando-o como uma nova personalização do Excel para a exibição.



Apenas os utilizadores com a função Administrador de aplicações ou Administrador de armazenamento podem ver o ícone de eliminação, alterar ou eliminar uma vista, ou alterar ou eliminar um relatório agendado.

## Tipos de relatórios

Esta tabela fornece uma lista abrangente das visualizações e páginas de inventário que estão disponíveis como relatórios que você pode personalizar, baixar e agendar.

### Relatórios do Active IQ Unified Manager

Tipo	Objeto de storage ou rede
Capacidade	Clusters Agregados Volumes Qtrees

Tipo	Objeto de storage ou rede
Saúde	Clusters Nós Agregados VMs de storage Volumes Compartilhamentos SMB/CIFS Compartilhamentos NFS
Desempenho	Clusters Nós Agregados VMs de storage Volumes LUNs Namespaces NVMe Interfaces de rede (LIFs) Portas
Qualidade do serviço	Grupos de políticas de QoS tradicionais Grupos de políticas de QoS adaptáveis Grupos de políticas de nível de Serviço de desempenho
Relações de proteção de volume (disponível na página volumes)	Todos os relacionamentos Último estado de transferência de 1 meses Último 1 mês taxa de transferência
Segurança	VMs de storage Clusters

## Limitações de relatórios

Existem algumas limitações com a nova funcionalidade de relatórios do Active IQ Unified Manager, das quais você deve estar ciente.

### Relatórios existentes de versões anteriores do Unified Manager

Você só pode editar a programação e os destinatários dos relatórios existentes que foram criados e importados (como arquivos .rptdesign) no Unified Manager 9,5 e versões anteriores. Se você personalizou qualquer um dos relatórios padrão fornecidos com o Unified Manager 9,5 ou anterior, esses relatórios personalizados não serão importados para a nova ferramenta de relatórios.

Se você precisar editar relatórios existentes importados de arquivos .rptdesign, siga um destes procedimentos e remova o relatório importado:

- criar uma nova visualização e agendar um relatório a partir dessa visualização (preferencial)
- Passe o Mouse sobre o relatório, copie o SQL e puxe os dados usando uma ferramenta externa

As visualizações padrão podem ser geradas como relatórios sem a necessidade de qualquer personalização. Você pode usar a nova solução de relatórios para recriar todos os relatórios personalizados.

### Agendar e relatar relacionamento

Você pode criar muitas agendas diferentes com qualquer combinação de destinatários para cada relatório salvo. No entanto, não é possível reutilizar a programação para vários relatórios.

### Relatório de proteção

Qualquer usuário com as permissões apropriadas pode editar ou excluir relatórios. Não há nenhuma maneira de impedir que outros usuários removam ou façam alterações em visualizações ou programações salvas.

### Relatórios de eventos

Embora você possa personalizar a exibição de eventos e fazer o download do relatório resultante no formato CSV, não é possível agendar relatórios de eventos recorrentes para geração e distribuição.

### Anexos de relatório

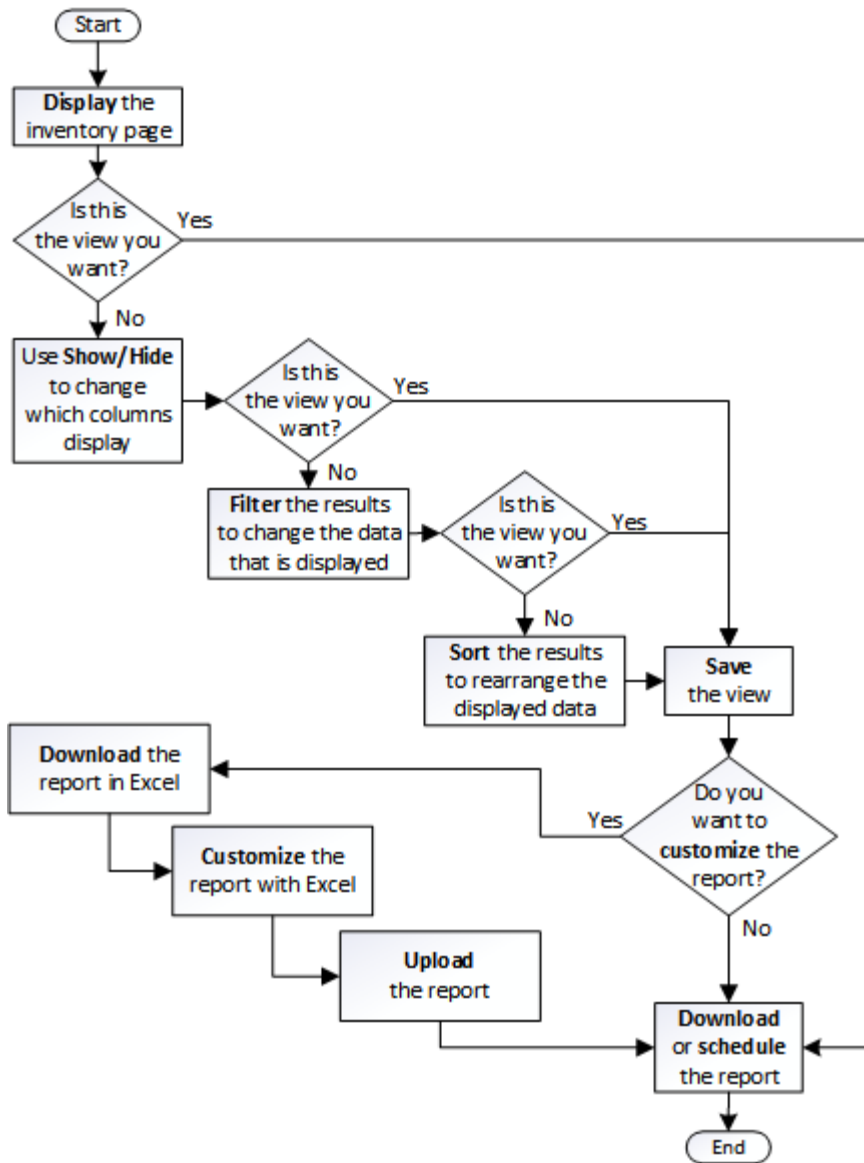
Os relatórios não podem ser enviados no corpo de um e-mail. Em vez disso, os relatórios são enviados apenas como anexos PDF, Excel ou CSV.

## Trabalhando com relatórios

Saiba como encontrar e personalizar visualizações de página de inventário em relatórios programados compartilháveis.

### Fluxo de trabalho do relatório

Árvore de decisão que descreve o fluxo de trabalho do relatório.



## Criação de relatórios de início rápido

Crie um relatório personalizado de amostra para experimentar a exploração de visualizações e relatórios de agendamento. Esse relatório de início rápido encontra uma lista de volumes que você pode querer migrar para a categoria de nuvem porque há uma quantidade razoável de dados inativos (frios). Você abrirá a exibição desempenho: Todos os volumes, personalizará a exibição usando filtros e colunas, salvará a exibição personalizada como um relatório e agendará o relatório para compartilhar uma vez por semana.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você precisa ter agregados FabricPool configurados e ter volumes nesses agregados.

Siga os passos abaixo para:

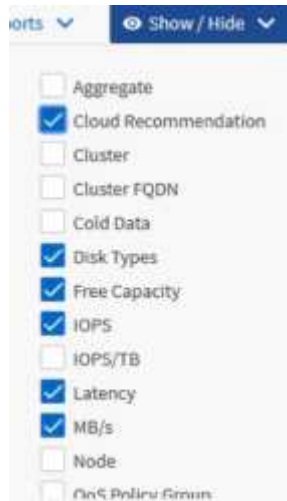
- Abra a vista predefinida



- Personalize as colunas filtrando e classificando os dados
- Guarde a vista
- Agende um relatório a ser gerado para a visualização personalizada

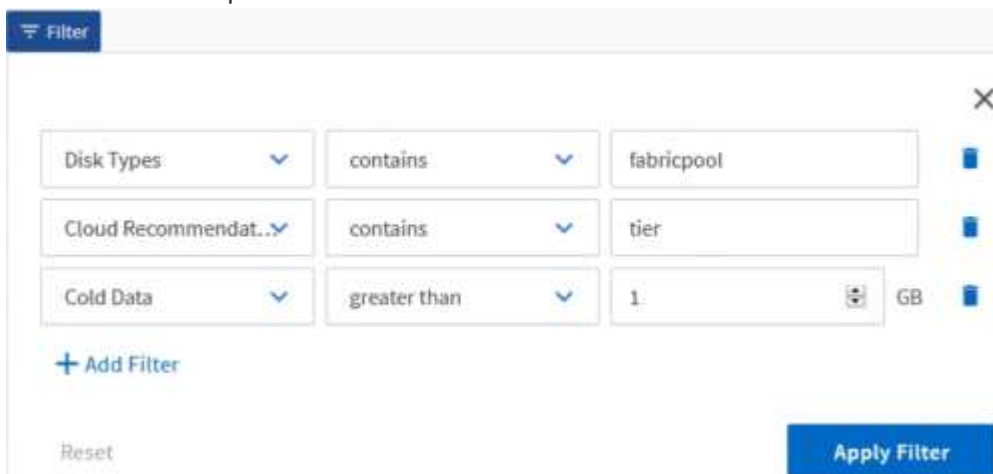
## Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **desempenho > todos os volumes**.
3. Clique em **Mostrar/Ocultar** para se certificar de que a coluna "tipos de disco" aparece na exibição.



Adicione ou remova outras colunas para criar um modo de exibição que contenha os campos importantes para o relatório.

4. Arraste a coluna "tipos de disco" ao lado da coluna "Recomendação de nuvem".
5. Clique no ícone de filtro para adicionar os três filtros a seguir e clique em **Apply Filter**:
  - Os tipos de disco contêm FabricPool
  - A recomendação de nuvem contém nível
  - Dados inativos superiores a 10 GB



Observe que cada filtro é associado a um lógico E que todos os volumes retornados devem atender a todos os critérios. Você pode adicionar um máximo de cinco filtros.

- Clique na parte superior da coluna dados inativos para classificar os resultados para que os volumes com os dados mais inativos apareçam na parte superior da exibição.
- Quando a vista é personalizada, o nome da vista é Unsaved View (Vista não guardada). Nomeie a exibição para refletir o que a exibição está mostrando, por exemplo, "Vols Change Tiering policy". Quando terminar, clique na marca de seleção ou pressione **Enter** para salvar a exibição com o novo nome.

Volumes - Performance / Vols change tiering policy ⓘ Last updated: Feb 8, 2019, 12:26 PM 🔄

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View: Vols change tiering policy 🔽 Search Volumes 🔍

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Reports 🔽 Show/Hide 🔽

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
rfa_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagnfsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

- Faça o download do relatório como um arquivo \* CSV\*, \* Excel\* ou \* PDF\* para ver a saída antes de programá-lo ou compartilhá-lo.

Abra o arquivo com um aplicativo instalado, como Microsoft Excel (CSV ou Excel) ou Adobe Acrobat (PDF), ou salve o arquivo.



Você pode personalizar ainda mais seu relatório usando filtros complexos, classificações, tabelas dinâmicas ou gráficos baixando a exibição como um arquivo do Excel. Depois de abrir o arquivo no Excel, use os recursos avançados para personalizar o relatório. Quando estiver satisfeito, carregue o ficheiro Excel. Este ficheiro, com as suas personalizações, é aplicado à vista quando o relatório é executado.

Para obter mais informações sobre como personalizar relatórios usando o Excel, consulte *exemplos de relatórios do Microsoft Excel*.

- Clique no botão **relatórios programados** na página de inventário. Todos os relatórios programados relacionados ao objeto, neste caso volumes, aparecem na lista.

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports

Volumes - Scheduled Reports View all Scheduled Reports

Add Schedule

Schedule Name	View	Recipients	Frequency	Format	
Weekly / Vols c... tiering policy	Performance / V... tiering policy	user@company.com	Weekly - Monday 1:00 PM	CSV	⋮

- Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.
- Introduza um nome para o relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

O seguinte relatório de exemplo está no formato CSV:

Status	Volume	Volume Id	Tiering Policy	Cold Data	Free Capacity	Total Capacity	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id
Ok	kjagnfsdst	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040
Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141

O seguinte relatório de amostra está em formato PDF:

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok	kjagnfsdst	Snapshot	28.01	121.32	150	ocum-mo	ocum-mo	aggr5_vs
Ok	nfs_vol4	Snapshot	379.64	2676.57	3072	ocum-mo	ocum-mo	aggr4

Com base nos resultados mostrados no relatório, você pode querer usar o Gerenciador de sistema do ONTAP ou a CLI do ONTAP para alterar a política de disposição em categorias para "auto" ou "all" de certos volumes para descarregar mais dados inativos na camada de nuvem.

## Procurar um relatório agendado

Você pode pesquisar relatórios programados por nome, nome de exibição, tipo de objeto ou destinatários.

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento > horários de relatórios**.
2. Use o campo de texto **pesquisar relatórios programados**.

Para encontrar relatórios por ...	Tente ...
Nome da programação	Digite parte do nome da programação do relatório.
Nome da vista	Digite parte do nome da exibição do relatório. As vistas padrão e as vistas personalizadas são apresentadas na lista de vistas.
Destinatário	Digite parte do endereço de e-mail.
Tipo de ficheiro	Digite "PDF", "CSV" ou "XLSX".

3. Você pode clicar no cabeçalho de uma coluna para classificar os relatórios em ordem crescente ou decrescente por essa coluna, como nome ou formato da programação.

## Personalizar relatórios

Há muitas maneiras de personalizar as exibições para criar um relatório que contenha todas as informações necessárias para gerenciar os clusters do ONTAP.

Comece com uma página de inventário padrão ou uma exibição personalizada e, em seguida, personalize-a adicionando ou removendo colunas, alterando a ordem da coluna, filtrando os dados ou classificando em uma

coluna específica em ordem ascendente ou decendente.

A partir do Unified Manager 9,8, você também pode baixar a exibição no Excel para personalizá-la usando recursos avançados. Quando terminar, carregue o ficheiro Excel personalizado. Se você agendar um relatório usando essa exibição, ele usará o arquivo Excel personalizado para criar relatórios robustos que você pode compartilhar.

Para obter mais informações sobre como personalizar relatórios usando o Excel, consulte *exemplos de relatórios do Microsoft Excel*.



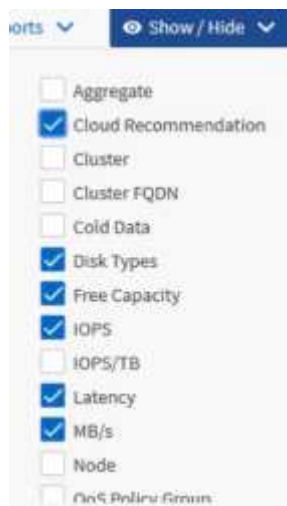
Você deve ter a função Administrador de aplicativos ou Administrador de armazenamento para gerenciar relatórios.

## Personalizar colunas

Use **Mostrar/Ocultar** para escolher as colunas que deseja usar no relatório. Arraste as colunas na página de inventário para reorganizá-las.

### Passos

1. Clique em **Mostrar/Ocultar** para adicionar ou remover colunas.



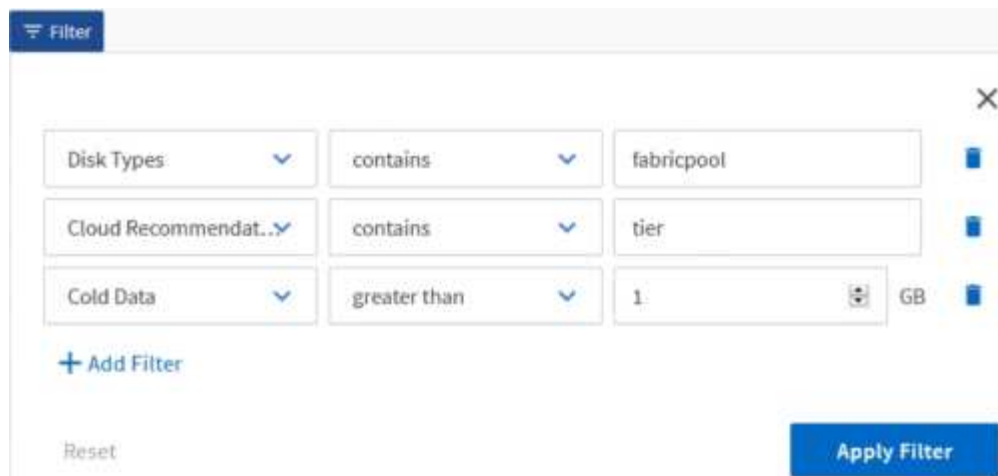
2. Na página de inventário, arraste colunas para reorganizá-las na ordem desejada no relatório.
3. Atribua um nome à vista não guardada para guardar as alterações.

## Filtragem de dados

Filtre os dados para garantir que os resultados correspondem aos requisitos do relatório. A filtragem permite exibir apenas os dados nos quais você está interessado.

### Passos

1. Clique no ícone de filtro para adicionar filtros para focar os resultados que deseja exibir e clique em **aplicar filtro**.



2. Atribua um nome à vista não guardada para guardar as alterações.

### Ordenar dados

Para classificar os resultados, clique em uma coluna e indique a ordem ascendente ou descendente. A classificação de dados prioriza as informações necessárias para o relatório.

#### Passos

1. Clique na parte superior de uma coluna para classificar os resultados para que as informações mais importantes sejam exibidas na parte superior da exibição.
2. Atribua um nome à vista não guardada para guardar as alterações.

### Usando a pesquisa para refinar sua visualização

Depois de ter a visualização desejada, você pode refinar ainda mais os resultados usando o campo pesquisar para se concentrar nos resultados que deseja incluir no relatório.

#### Passos

1. Abra o modo de exibição personalizado ou padrão que você deseja usar como base do relatório.
2. Digite o campo pesquisar para refinar os dados listados na exibição. Pode introduzir dados parciais em qualquer uma das colunas apresentadas. Por exemplo, se você quiser pesquisar nós que incluem "US\_East" no nome, você pode refinar a lista completa de nós.

Os resultados da pesquisa são salvos na exibição personalizada e usados no relatório agendado resultante.

3. Atribua um nome à vista não guardada para guardar as alterações.

### Usando o Excel para personalizar seu relatório

Depois de salvar a exibição, você pode baixá-la no formato Excel Workbook (.xlsx). Ao abrir o arquivo Excel, você pode usar recursos avançados do Excel para personalizar o relatório.

## Antes de começar

Você só pode carregar um arquivo do Excel Workbook com a extensão .xlsx.

Por exemplo, alguns recursos avançados do Excel que você pode usar no relatório incluem:

- Ordenação de várias colunas
- Filtragem complexa
- Tabelas dinâmicas
- Gráficos

- O ficheiro Excel transferido utiliza o nome de ficheiro predefinido para a vista, não o nome guardado.
  - O formato é <View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx.
  - Por exemplo, um modo de exibição personalizado salvo chamado `Volumes-not online` tem um nome de arquivo de `health-volumes-05-May-2020-19-18-00.xlsx` se salvo naquele dia e hora.
- Pode adicionar folhas ao ficheiro Excel, mas não alterar folhas existentes.
  - Não altere as folhas, dados e informações existentes. Em vez disso, copie os dados para uma nova página que você criar.
  - Uma exceção à regra acima é que você pode criar fórmulas na página "data". Use as fórmulas da página de dados para criar gráficos em novas páginas.
  - Não atribua um nome a uma nova folha de dados ou informações.
- Se existir um ficheiro Excel personalizado, existe uma marca de verificação ao lado do item de menu **relatórios > carregar Excel**. Ao baixar o arquivo do Excel, a versão com as



personalizações é usada.



## Passos

1. Abra o modo de exibição padrão, personalizado ou salvo que você deseja usar como base do relatório.
2. Selecione **relatórios > Download Excel**.
3. Salve o arquivo. O ficheiro é guardado na pasta de transferências.
4. Abra o arquivo salvo no Excel. Não mova o arquivo para um novo local ou, se você fizer seu trabalho em outro local, salve o arquivo de volta para o local original usando o nome do arquivo original antes de fazer o upload do arquivo.
5. Personalize o arquivo usando recursos do Excel, como tipos complexos, filtros em camadas, tabelas dinâmicas ou gráficos. Para obter mais informações, consulte a documentação do Microsoft Excel.

6. Selecione **relatórios** > **carregar Excel** e selecione o ficheiro que modificou. O arquivo baixado mais recentemente é carregado a partir do mesmo local do arquivo.
7. Envie um relatório de teste usando o recurso **relatórios programados**.

## A transferir relatórios

Você pode baixar relatórios e salvar os dados em uma unidade local ou de rede como um arquivo CSV (valores separados por vírgulas), um arquivo do Microsoft Excel (.XLSX) ou um arquivo PDF. Você pode abrir arquivos CSV e XLSX com aplicativos de Planilha, como o Microsoft Excel, e arquivos PDF com leitores como o Adobe Acrobat.

### Passos

1. Clique no botão **relatórios** para fazer o download do relatório como um dos seguintes:

Escolha	Para...
Faça o download da CSV	Salve o relatório como um arquivo CSV (valores separados por vírgula).
Faça o download da PDF	Salve o relatório como um arquivo .pdf.
Baixe o Excel	Salve o relatório como um arquivo do Microsoft Excel (XLSX).

## Agendar relatórios

Depois de ter uma exibição que deseja reutilizar e compartilhar como um relatório, você pode programá-la usando o Active IQ Unified Manager. Você pode gerenciar relatórios programados, alterar os destinatários e a frequência de distribuição para cada agendamento de relatório.

Você pode agendar a maioria das visualizações ou páginas de inventário no Unified Manager. Exceções são eventos, que são relatórios que você pode baixar como arquivos CSV, mas você não pode agendar eventos para regeneração e compartilhamento. Você também não pode baixar ou agendar os painéis, favoritos ou páginas de configuração.

A partir do Active IQ Unified Manager 9,8, você pode baixar visualizações no formato Microsoft Excel e personalizá-las. Você pode usar recursos avançados do Excel, como sortes complexos, filtros em camadas, tabelas dinâmicas e gráficos. Quando estiver satisfeito com o relatório do Excel resultante, você pode fazer o upload do arquivo do Excel para uso sempre que o relatório for agendado e compartilhado.

Você pode agendar as visualizações incorporadas ou exibições personalizadas. Você pode escolher qual tipo de arquivo enviar, seja CSV, PDF ou XSLX. Quando você agendar um relatório pela primeira vez, você pode baixá-lo e atribuir-se como o único destinatário para ver o relatório como seus destinatários o verão.

### Agendar um relatório

Depois de ter um arquivo de exibição ou Excel que você deseja agendar para geração e

distribuição regulares, você pode agendar o relatório.

### Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado as configurações do servidor SMTP na página **Geral > notificações** para que o mecanismo de relatórios possa enviar relatórios como anexos de e-mail para a lista de destinatários do servidor Unified Manager.
- O servidor de e-mail deve estar configurado para permitir que anexos sejam enviados com os e-mails gerados.

Use as etapas a seguir para testar e agendar um relatório a ser gerado para uma exibição. Selecione ou personalize a vista que pretende utilizar. O procedimento a seguir usa uma exibição de rede que mostra o desempenho de suas interfaces de rede, mas você pode usar qualquer exibição desejada.

### Passos

1. Abra a vista. Este exemplo usa a exibição de rede padrão que mostra o desempenho de LIF. No painel de navegação esquerdo, clique em **rede > interfaces de rede**.
2. Personalize a exibição conforme necessário usando os recursos integrados do Unified Manager.
3. Depois de personalizar a exibição, você pode fornecer um nome exclusivo no campo **Exibir** e clicar na marca de seleção para salvá-la.



4. Você pode usar os recursos avançados do Microsoft Excel para personalizar seu relatório. Para obter detalhes, "[Usando o Excel para personalizar seu relatório](#)" consulte .
5. Para ver a saída antes de programá-la ou compartilhá-la:

Opção	Descrição
<b>Se você usou o Excel para personalizar o relatório</b>	Ver o ficheiro Excel transferido existente.
<b>Se você não usou o Excel para personalizar o relatório</b>	Faça o download do relatório como um arquivo <b>CSV</b> , <b>PDF</b> ou <b>XLSX</b> .

Abra o arquivo com um aplicativo instalado, como Microsoft Excel (CSV/XSLX) ou Adobe Acrobat (PDF).

6. Se estiver satisfeito com o relatório, clique em **relatórios programados**.
7. Na página Agenda de relatórios, clique em **Adicionar programação**.
8. Aceite o nome padrão, que é uma combinação do nome da vista e da frequência, ou personalize o **nome da programação**.
9. Para testar o relatório agendado pela primeira vez, adicione-se apenas como **destinatário**. Quando estiver satisfeito, adicione os endereços de e-mail para todos os destinatários do relatório.
10. Especifique com que frequência o relatório será gerado e enviado aos destinatários. Você pode escolher **Daily**, **Weekly** ou **Monthly**.
11. Selecione o formato **PDF**, **CSV** ou **XSLX**.





Para relatórios em que você usou o Excel para personalizar o conteúdo, selecione sempre **XSLX**.

12. Clique na marca de seleção (✓) para salvar a programação do relatório.

LIFs - Scheduled Reports [View all Scheduled Reports](#)

[Add Schedule](#)

Schedule Name	View	Recipients	Frequency	Format
Weekly / LIF performar	Performance / LIF pe ▼	test@netapp.com	Weekly ▼ Thursda ▼ 4:30 PM ▼	PDF ▼

✓ ✕

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência programada.

### Programação de relatórios .rptdesign importados

Você pode agendar relatórios existentes que foram criados e importados em uma versão anterior do Unified Manager.

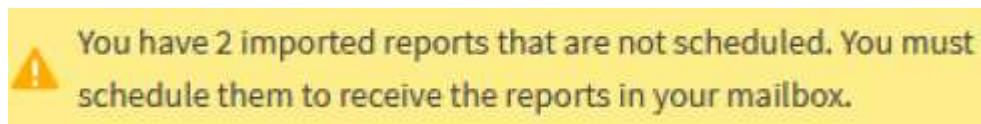
A programação de relatórios importados requer o seguinte:

- Relatórios de arquivo .rptdesign criados pelo BIRT importados em uma versão anterior do Unified Manager
- Aplicável ao atualizar para o Unified Manager 9,6 GA ou posterior

Depois de atualizar para o Unified Manager 9,6 GA ou posterior, a página Agenda de relatórios lista os relatórios importados. Você pode editar a programação desses relatórios para especificar os endereços de e-mail do destinatário, a frequência e o formato (PDF ou CSV). Caso contrário, esses relatórios não podem ser editados ou visualizados na IU do Unified Manager.

### Passos

1. Abra a página Agenda de relatórios. Se você tiver importado relatórios, uma mensagem será exibida.



2. Clique no nome **View** para exibir a consulta SQL que está sendo usada para gerar o relatório.

**Imported Report**

This report is generated using following database query:

```
SELECT c.name AS 'Cluster', m.name AS 'SVM', v.name AS 'Volume', s.name AS 'Share',
s.path AS 'Path', q.name AS 'Qtree', s.shareProperties AS 'Properties', a.userOrGroup
AS 'User', a.permission AS 'Permission' FROM ocum_report.cifsshare s JOIN
ocum_report.cifsshareacl a ON s.id = a.cifsShareId JOIN ocum_report.cluster c ON
s.clusterId = c.id JOIN ocum_report.svm m ON s.svmId = m.id JOIN
ocum_report.volume v ON s.volumeId = v.id JOIN ocum_report.qtree q ON s.qtreeId =
q.id
```

3. Clique no ícone mais , clique em **Editar**, defina os detalhes da programação do relatório e salve o relatório.



Você também pode excluir quaisquer relatórios indesejados do ícone mais .

## Gerenciamento de programações de relatórios

Você pode gerenciar suas programações de relatórios na página agendas de relatórios. Você pode exibir, modificar ou excluir programações existentes.



### Antes de começar



Não é possível programar novos relatórios a partir da página agendas de relatórios. Você só pode adicionar relatórios programados das páginas de inventário de objetos.

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

### Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento > horários de relatórios**.
2. Na página Agenda de relatórios:

Se você quiser...	Então...
Ver uma agenda existente	Percorra a lista de relatórios existentes utilizando as barras de deslocamento e os controles de página.

Se você quiser...	Então...
Editar uma agenda existente	<ol style="list-style-type: none"> <li>Clique no ícone mais  da agenda que deseja usar.</li> <li>Clique em <b>Editar</b>.</li> <li>Faça as alterações necessárias.</li> <li>Clique na marca de verificação para guardar as alterações.</li> </ol>
Eliminar uma agenda existente	<ol style="list-style-type: none"> <li>Clique no ícone mais  da agenda que deseja usar.</li> <li>Clique em <b>Excluir</b>.</li> <li>Confirme a sua decisão.</li> </ol>

## Editar relatórios programados

Depois que os relatórios forem agendados, você poderá editá-los na página Agenda de relatórios.

### Antes de começar

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

### Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento > horários de relatórios**.


#### Scheduled Reports

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	<a href="#">Performance / Tom_test</a>	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	<a href="#">Health / my view</a>	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	<a href="#">Performance / LIF performance</a>	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



Se você tiver as permissões apropriadas, você pode alterar qualquer relatório e sua programação no sistema.

2. Clique no ícone mais  da agenda que deseja alterar.
3. Clique em **Editar**.
4. Você pode alterar a lista **Nome da programação, destinatário, frequência e formato** para a programação do relatório.

5. Quando terminar, clique na marca de verificação para guardar as alterações.

## Eliminar relatórios programados

Depois que os relatórios forem agendados, você poderá excluí-los da página Agenda de relatórios.

### Antes de começar

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

### Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento > horários de relatórios**.


#### Scheduled Reports

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	<a href="#">Performance / Tom_test</a>	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	<a href="#">Health / my view</a>	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	<a href="#">Performance / LIF performance</a>	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



Se você tiver as permissões apropriadas, poderá remover qualquer relatório e sua programação no sistema.

2. Clique no ícone mais  da agenda que deseja remover.
3. Clique em **Excluir**.
4. Confirme a sua decisão.

O relatório agendado é removido da lista e não será mais gerado e distribuído na programação definida.



Se você excluir uma exibição personalizada da página de inventário, todos os arquivos personalizados do Excel ou relatórios programados que usam essa exibição também serão excluídos.

## Exemplos de relatórios personalizados

Esses exemplos de relatórios personalizados são comumente usados para ajudá-lo a identificar possíveis problemas e responder a possíveis problemas antes que ocorram.

A lista de relatórios nesta seção não é exaustiva e crescerá ao longo do tempo. Você pode sugerir relatórios personalizados para adicionar a esta seção fornecendo feedback de documentação.



Você deve ter a função Administrador de aplicativos ou Administrador de armazenamento para gerenciar relatórios.

## Personalizar relatórios de armazenamento de cluster

Os exemplos de relatórios de armazenamento de cluster nesta seção são apenas exemplos para ajudá-lo a entender como criar relatórios sobre a capacidade do cluster para ajudá-lo a monitorar os recursos do sistema de armazenamento.

### Criando um relatório para exibir a capacidade por modelo de cluster

É possível criar um relatório para analisar a capacidade de storage e a utilização de clusters com base no modelo de sistema de storage.

#### Antes de começar

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

Siga as etapas a seguir para criar uma exibição personalizada que exiba a capacidade por modelo de cluster e, em seguida, agende um relatório a ser gerado para essa exibição.

#### Passos

1. No painel de navegação esquerdo, clique em **Storage > clusters**.
2. No menu Exibir, selecione **capacidade > todos os clusters**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas, como "Cluster FQDN" e "versão do sistema operacional", que você não deseja no relatório.
4. Arraste a "capacidade bruta total", o "modelo/família" e as três colunas agregadas perto da coluna "Cluster".
5. Clique na parte superior da coluna "modelo/Família" para classificar os resultados por tipo de cluster.
6. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, "capacidade por modelo de cluster".
7. Clique no botão **relatórios programados** na página de inventário.
8. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página **Report Schedules** para que você possa definir as características de agendamento para o novo relatório.
9. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer adicionar mais capacidade a determinados clusters ou atualizar modelos de cluster mais antigos.

### Criação de um relatório para identificar clusters com a capacidade LUN mais não alocada

Você pode criar um relatório para localizar os clusters com a capacidade LUN mais não alocada, maior que .5 TB, para ajudar a identificar onde é possível adicionar cargas de trabalho adicionais.

## Antes de começar

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

Use as etapas a seguir para criar uma exibição personalizada que exiba clusters com a capacidade LUN mais não alocada e, em seguida, programe um relatório a ser gerado para essa exibição.

## Passos

1. No painel de navegação esquerdo, clique em **Storage > clusters**.
2. No menu Exibir, selecione **capacidade > todos os clusters**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Arraste a coluna "capacidade LUN não alocada" perto da coluna "par de HA".
5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Apply Filter**:
  - Capacidade LUN não alocada superior a 0,5 TB
6. Clique na parte superior da coluna "capacidade LUN não alocada" para classificar os resultados pela maior quantidade de capacidade LUN não alocada.
7. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo ""capacidade LUN não alocada mais"" e clique na marca de seleção (✓).
8. Clique no botão **relatórios programados** na página de inventário.
9. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.
10. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira usar a capacidade de LUN não alocada do cluster.

## Criação de um relatório para visualizar pares de HA com a maior capacidade disponível

É possível criar um relatório para localizar os pares de alta disponibilidade (HA) com mais capacidade para provisionar novos volumes e LUNs.

## Antes de começar

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

Siga as etapas a seguir para criar uma visualização personalizada que exiba pares de HA classificados pela capacidade mais disponível para provisionar novos volumes e LUNs e, em seguida, agendar um relatório para ser gerado para essa visualização.

## Passos

1. No painel de navegação esquerdo, clique em **Storage > clusters**.
2. No menu Exibir, selecione **capacidade > todos os clusters**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Arraste a coluna "agregar capacidade não utilizada" perto da coluna "par de HA".

5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Apply Filter**:
  - Capacidade agregada não utilizada superior a 0,5 TB
6. Clique na parte superior da coluna "agregar capacidade não utilizada" para classificar os resultados pela maior quantidade de capacidade agregada não utilizada.
7. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, ""capacidade agregada menos usada"" e clique na marca de seleção (✓).
8. Clique no botão **relatórios programados** na página de inventário.
9. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.
10. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira equilibrar pares de HA com base na capacidade agregada.

### **Criando um relatório para exibir nós que executam versões mais antigas do ONTAP**

Você pode criar um relatório para exibir a versão do software ONTAP instalada em todos os nós de cluster para que você possa ver quais nós deve atualizar.

#### **Antes de começar**

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

Use as etapas a seguir para criar uma exibição personalizada que exiba nós executando versões mais antigas do ONTAP e, em seguida, programe um relatório a ser gerado para essa exibição.

#### **Passos**

1. No painel de navegação esquerdo, clique em **Storage > Nodes**.
2. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
3. Arraste a coluna "versão do sistema operacional" perto da coluna "nó".
4. Clique na parte superior da coluna "versão do sistema operacional" para classificar os resultados pela versão mais antiga do ONTAP.
5. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, ""nodes by ONTAP version"".
6. Clique no botão **relatórios programados** na página de inventário.
7. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.
8. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer atualizar os nós que executam versões mais antigas do ONTAP.

## Personalização de relatórios de capacidade agregada

Esses relatórios personalizados de amostra são usados para ajudá-lo a identificar e responder a possíveis problemas relacionados à capacidade de armazenamento agregado.

Os relatórios nesta seção são apenas exemplos para ajudá-lo a entender como criar relatórios sobre capacidade agregada para ajudá-lo a monitorar os recursos do sistema de armazenamento.

### Criação de um relatório para visualizar agregados que atingem a capacidade total

Você pode criar um relatório para localizar os agregados que estão atingindo a capacidade máxima para adicionar mais capacidade ou mover workloads para outros agregados.

#### Antes de começar

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

Use as etapas a seguir para criar uma exibição personalizada que exiba agregados que atingem a capacidade total e, em seguida, agende um relatório a ser gerado para essa exibição.

#### Passos

1. No painel de navegação à esquerda, clique em **Storage > Aggregates**.
2. No menu Exibir, selecione **capacidade > todos os agregados**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Apply Filter**:
  - Dias para completar menos de 45 dias
5. Clique na parte superior da coluna ""dias a cheio"" para classificar os resultados pelo menor número de dias restantes para alcançar a capacidade total.
6. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, ""dias para capacidade agregada total"" e clique na marca de seleção (✓).
7. Clique no botão **relatórios programados** na página de inventário.
8. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página **Report Schedules** para que você possa definir as características de agendamento para o novo relatório.
9. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer aumentar o storage em agregados que alcançam a capacidade total. Além disso, você pode querer aumentar o limite dias até capacidade total para mais do que os 7 dias padrão para receber eventos que fornecem mais tempo para reagir ao espaço ficando baixo em agregados.



## Criar um relatório para visualizar agregados que estejam 80% ou mais completos

Você pode criar um relatório para destacar os agregados que estão 80% ou mais completos.

### Antes de começar

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

Use as etapas a seguir para criar uma exibição personalizada que exiba agregados que estejam 80% ou mais completos e, em seguida, programe um relatório a ser gerado para essa exibição.

### Passos

1. No painel de navegação à esquerda, clique em **Storage > Aggregates**.
2. No menu Exibir, selecione **capacidade > todos os agregados**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Arraste as colunas "Available Data %" e "Used Data %" perto da coluna "Aggregate".
5. Clique no ícone de filtro, adicione os seguintes filtros e clique em **Apply Filter**:
  - A % de dados utilizados é superior a 80%
6. Clique na parte superior da coluna "dados usados %" para classificar os resultados por porcentagem de capacidade.
7. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, "agregados próximos" e clique na marca de seleção (✓).
8. Clique no botão **relatórios programados** na página de inventário.
9. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.
10. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer mover alguns dados de certos agregados.

## Criando um relatório para visualizar agregados que estão sobrecomprometidos

Você pode criar um relatório para analisar a capacidade de storage e o uso de agregados e visualizar agregados com excesso de comprometimento.

### Antes de começar

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

Use as etapas a seguir para criar uma exibição personalizada que exiba agregados que estejam excedendo o limite de comprometimento excessivo e, em seguida, programe um relatório a ser gerado para essa exibição.

### Passos

1. No painel de navegação à esquerda, clique em **Storage > Aggregates**.

2. No menu Exibir, selecione **capacidade > todos os agregados**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Arraste a coluna ""capacidade excedentária %"" perto da coluna ""agregado"".
5. Clique no ícone de filtro, adicione os seguintes filtros e clique em **Apply Filter**:
  - Capacidade excedentária % é superior a 100%
6. Clique na parte superior da coluna "capacidade supercomprometida" para classificar os resultados por porcentagem de capacidade.
7. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, ""agregados sobrecomprometidos"" e clique na marca de seleção (✓).
8. Clique no botão **relatórios programados** na página de inventário.
9. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.
10. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer adicionar mais capacidade a agregados ou mover alguns dados de certos agregados.

## Personalizar relatórios de capacidade de volume

Esses relatórios personalizados de amostra são usados para ajudá-lo a identificar e responder a possíveis problemas relacionados à capacidade de volume e desempenho.

### Criação de um relatório para identificar volumes que estão próximos de capacidade total que têm o Snapshot Autodelete desativado

Você pode criar um relatório que contenha a lista de volumes que estão se aproximando da capacidade total com o recurso Snapshot Autodelete desativado. Os resultados podem ajudar a identificar volumes onde você pode querer configurar o Snapshot Autodelete.

#### Antes de começar

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

Siga as etapas abaixo para criar uma exibição personalizada que exiba as colunas necessárias na ordem correta e, em seguida, programe um relatório a ser gerado para essa exibição.

#### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **capacidade > todos os volumes**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Arraste e solte as colunas "Snapshot Autodelete" e "Days to Full" perto da coluna "Available Data Capacity" (capacidade de dados disponível).

5. Clique no ícone de filtro, adicione os dois filtros a seguir e clique em **Apply Filter**:
  - Dias para completar menos de 30 dias
  - O Snapshot Autodelete está desativado
6. Clique na parte superior da coluna **Days to Full** para que os volumes com o menor número de dias restantes apareçam no topo da lista.
7. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo ""Vols near Capacity"".
8. Clique no botão **relatórios programados** na página de inventário.
9. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer habilitar o Snapshot Autodelete nos volumes ou encontrar uma maneira de aumentar o espaço disponível.

### **Criação de um relatório para identificar o espaço usado por volumes com thin Provisioning desativado**

Quando um volume não é thin Provisioning, ele ocupa a quantidade total de espaço no disco, conforme definido quando o volume foi criado. A identificação de volumes com thin Provisioning desativado ajuda a decidir se deseja ativar o thin Provisioning em determinados volumes.

#### **Antes de começar**

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

Siga as etapas abaixo para criar uma exibição personalizada que exiba as colunas necessárias na ordem correta e, em seguida, programe um relatório a ser gerado para essa exibição.

#### **Passos**

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **capacidade > todos os volumes**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Arraste e solte as colunas ""Used Data %" e as colunas "thin Provisioning" perto da coluna "Available Data Capacity" (capacidade de dados disponível).
5. Clique no ícone de filtro, adicione o seguinte filtro, **thin Provisioning é no** e clique em **Apply Filter**.
6. Clique na parte superior da coluna "dados usados %" para classificar os resultados de modo que os volumes com a porcentagem mais alta apareçam no topo da lista.
7. Salve a exibição com um nome para refletir o que a exibição está mostrando, por exemplo ""Vols no thin Provisioning"".
8. Clique no botão **relatórios programados** na página de inventário.
9. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página **Report Schedules** para que você possa definir as características de agendamento para o novo relatório.
10. Digite um nome para a programação do relatório e preencha os outros campos do relatório e clique na marca de seleção (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer habilitar o provisionamento de thin Provisioning em determinados volumes.

### **Criar um relatório para identificar volumes em agregados FabricPool que devem migrar dados para a camada de nuvem**

Você pode criar um relatório que contenha a lista de volumes que atualmente residem em agregados FabricPool, que tenham uma recomendação de nuvem de categoria e que tenham uma grande quantidade de dados inativos. Este relatório pode ajudá-lo a decidir se você deve alterar a política de disposição em categorias de certos volumes para "auto" ou "all" para descarregar mais dados inativos (inativos) para a camada de nuvem.

#### **Antes de começar**

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você precisa ter agregados FabricPool configurados e ter volumes nesses agregados.

Siga as etapas abaixo para criar uma exibição personalizada que exiba as colunas necessárias na ordem correta e, em seguida, programe um relatório a ser gerado para essa exibição.

#### **Passos**

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **desempenho > todos os volumes**.
3. No seletor de colunas, certifique-se de que a coluna "Disk Type" (tipo de disco) seja exibida na exibição.

Adicione ou remova outras colunas para criar uma exibição importante para o relatório.

4. Arraste e solte a coluna "Disk Type" (tipo de disco) perto da coluna "Cloud Recommendation" (Recomendação da nuvem).
5. Clique no ícone de filtro, adicione os três filtros a seguir e clique em **Apply Filter**:
  - Tipo de disco contém FabricPool
  - A recomendação de nuvem contém nível
  - Dados inativos superiores a 10 GB

6. Clique na parte superior da coluna dados inativos para que os volumes com mais dados inativos apareçam na parte superior da visualização.
7. Salve a exibição com um nome para refletir o que a exibição está mostrando, por exemplo, "Vols Change Tiering policy".

Volumes - Performance / Vols change tiering policy

Last updated: Feb 8, 2019, 12:26 PM

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View Vols change tiering policy  3

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
<a href="#">nfs_vol4</a>	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
<a href="#">kjagnfsdst</a>	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

8. Clique no botão **relatórios programados** na página de inventário.
9. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.
10. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer usar o Gerenciador de sistema ou a CLI do ONTAP para alterar a política de disposição em categorias para "auto" ou "all" para certos volumes para descarregar mais dados inativos na camada de nuvem.

## Personalizar relatórios de capacidade do Qtree

Esses relatórios personalizados de amostra são usados para ajudá-lo a identificar e responder a possíveis problemas relacionados à capacidade do Qtree.

### Criando um relatório para visualizar qtrees que estão quase cheios

Você pode criar um relatório para analisar a capacidade de armazenamento e a utilização de qtrees e para visualizar qtrees que estão quase cheios.

#### Antes de começar

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

Use as etapas a seguir para criar uma exibição personalizada que exiba qtrees quase cheios e, em seguida, programe um relatório a ser gerado para essa exibição.

#### Passos

1. No painel de navegação esquerdo, clique em **Storage > Qtrees**.
2. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
3. Arraste a coluna "Disk Used %" (disco usado %) perto da coluna "Qtrees".
4. Clique no ícone de filtro, adicione os seguintes filtros e clique em **Apply Filter**:
  - O disco utilizado % é superior a 75%
5. Clique na parte superior da coluna "disco usado %" para classificar os resultados por porcentagem de capacidade.
6. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, "Qtrees se aproximando completamente" e clique na marca de seleção (✓).
7. Clique no botão **relatórios programados** na página de inventário.
8. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página **Report Schedules** para que você possa definir as características de agendamento para o novo relatório.
9. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer ajustar os limites rígidos e flexíveis do disco (se definido), ou equilibrar os dados entre os qtrees.

## Personalizar relatórios de compartilhamento NFS

Você pode personalizar relatórios de compartilhamento NFS para analisar informações sobre políticas e regras de exportação de NFS para volumes em seus sistemas de storage. Por exemplo, você pode personalizar relatórios para exibir volumes com caminhos de montagem inacessíveis e volumes com a política de exportação padrão.

## Criando um relatório para exibir volumes que têm um caminho de montagem inacessível

Você pode criar um relatório para encontrar volumes que tenham um caminho de montagem inacessível.

### Antes de começar

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

Use as etapas a seguir para criar uma exibição personalizada para volumes que têm um caminho de montagem inacessível e, em seguida, agendar um relatório a ser gerado para essa exibição.

### Passos

1. No painel de navegação à esquerda, clique em **Storage > compartilhamentos NFS**.
2. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
3. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Apply Filter**:
  - O caminho de montagem ativo é não
4. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo ""volumes com um caminho de montagem inacessível"" e clique na marca de seleção (✓).
5. Clique no botão **relatórios programados** na página de inventário.
6. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.
7. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer corrigir os caminhos de montagem inacessíveis.

## Criando um relatório para exibir volumes que estão usando a política de exportação padrão

Você pode criar um relatório para localizar volumes que estejam usando a política de exportação padrão.

### Antes de começar

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

Siga as etapas a seguir para criar uma exibição personalizada para volumes que estejam usando a política de exportação padrão e, em seguida, agendar um relatório a ser gerado para essa exibição.

### Passos

1. No painel de navegação à esquerda, clique em **Storage > compartilhamentos NFS**.
2. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
3. Arraste a coluna ""Política de exportação"" perto da coluna "volume".
4. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Apply Filter**:

- Política de exportação contém padrão
5. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo ""volumes com uma política de exportação padrão"" e clique na marca de seleção (✓).
  6. Clique no botão **relatórios programados** na página de inventário.
  7. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.
  8. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira configurar uma política de exportação personalizada.

## Personalização de relatórios de VM de storage

Você pode criar relatórios de VM de storage para analisar informações de volume e visualizar a integridade geral e a disponibilidade de storage. Por exemplo, você pode criar relatórios para exibir SVMs atingindo a contagem máxima de volume e analisar SVMs paradas.

### Criação de um relatório para visualizar VMs de armazenamento atingindo o limite máximo de volume

Você pode criar um relatório para localizar SVMs que estão atingindo o limite máximo de volume.

#### Antes de começar

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

Siga as etapas a seguir para criar uma exibição personalizada que exiba VMs de armazenamento que estão atingindo o limite máximo de volume e, em seguida, agende um relatório a ser gerado para essa exibição.

#### Passos

1. No painel de navegação esquerdo, clique em **Storage > Storage VMs**.
2. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
3. Arraste as colunas "contagem de volume" e "volumes máximos permitidos" perto da coluna "Storage VM".
4. Clique na parte superior da coluna ""volumes máximos permitidos"" para classificar os resultados pelo maior número de volumes.
5. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo ""SVMs atingindo volumes máximos"" e clique na marca de seleção (✓).
6. Clique no botão **relatórios programados** na página de inventário.
7. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página **Report Schedules** para que você possa definir as características de agendamento para o novo relatório.
8. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.



O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira equilibrar os volumes atribuídos às VMs de storage ou, se possível, usar o Gerenciador de sistema do ONTAP para alterar o máximo de volumes permitidos.

## Criando um relatório para exibir VMs de armazenamento interrompidas

Você pode criar um relatório para exibir uma lista de todos os SVMs paradas.

### Antes de começar

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

Use as etapas a seguir para criar uma exibição personalizada que exiba VMs de armazenamento interrompidas e, em seguida, agende um relatório a ser gerado para essa exibição.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > Storage VMs**.
2. No menu Exibir, selecione **Saúde > todas as VMs de armazenamento**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Arraste a coluna "Estado" perto da coluna "Storage VM".
5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Apply Filter**:
  - Estado parado
6. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo "SVMs paradas" e clique na marca de seleção (✓).
7. Clique no botão **relatórios programados** na página de inventário.
8. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página **Report Schedules** para que você possa definir as características de agendamento para o novo relatório.
9. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer investigar por que o SVM está parado para ver se você deve reiniciar os SVMs parados.

## Personalizar relatórios de relacionamento de volume

O relatório Inventário de relacionamentos de volume permite analisar os detalhes do inventário de armazenamento em um cluster, entender o grau de proteção necessário para os volumes e filtrar os detalhes do volume com base na origem da falha, padrão e programações.

## Criar um relatório para agrupar relações de volume por origem da falha

Você pode criar um relatório que agrupa volumes pelo motivo pelo qual o relacionamento está em um estado não saudável.

### Antes de começar

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

Use as etapas a seguir para criar uma exibição personalizada que agrupe volumes por origem da falha e, em seguida, programe um relatório a ser gerado para essa exibição.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **relacionamento > todos os relacionamentos**.
3. Selecione **Mostrar/Ocultar** para se certificar de que as colunas ""Saúde do relacionamento"" e ""razão não saudável"" aparecem na exibição.

Adicione ou remova outras colunas para criar uma exibição importante para o relatório.

4. Arraste as colunas ""Saúde do relacionamento" e ""razão não saudável" perto da coluna ""Estado"".
5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Apply Filter**:
  - A saúde do relacionamento é ruim
6. Clique na parte superior da coluna "motivo não saudável" para agrupar as relações de volume por origem da falha.
7. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, "relacionamentos vol por falha".
8. Clique no botão **relatórios programados** na página de inventário.
9. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode investigar a origem e o impactos de cada tipo de falha.

## Criando um relatório para agrupar relacionamentos de volume por problema

Você pode criar um relatório que agrupa as relações de volume por problema.

### Antes de começar

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

Use as etapas a seguir para criar uma exibição personalizada que agrupa as relações de volume por problema e, em seguida, agende um relatório a ser gerado para essa exibição.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **relacionamento > todos os relacionamentos**.

3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Arraste a coluna "razão não saudável" perto da coluna "Estado".
5. Clique na parte superior da coluna "motivo não saudável" para agrupar os volumes por problema.
6. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, "relacionamentos vol por questão".
7. Clique no botão **relatórios programados** na página de inventário.
8. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode investigar a origem e o impactos de cada tipo de problema.

### **Criar um relatório para visualizar tendências de transferência de volume em intervalos de tempo específicos**

Você pode criar um relatório que exibe tendências de transferência de volume em intervalos de tempo específicos.

#### **Antes de começar**

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

Siga as etapas a seguir para criar uma exibição personalizada para volumes em intervalos de tempo específicos e, em seguida, agendar um relatório a ser gerado para essa exibição.

#### **Passos**

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **relacionamento > último Status da transferência de 1 meses**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Arraste a coluna duração da transferência perto da coluna "resultado operacional".
5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Apply Filter**:
  - Hora de fim da transferência nos últimos 7 dias
6. Clique na parte superior da coluna "duração da transferência" para classificar os volumes por intervalo de tempo.
7. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo "volumes por duração".
8. Clique no botão **relatórios programados** na página de inventário.
9. Insira um nome para a programação do relatório, defina a frequência como **semanal** e preencha os outros campos do relatório e, em seguida, clique na marca de seleção (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados apresentados no relatório, pode investigar os intervalos de tempo de transferência.

## A criação de um relatório para visualizar a transferência de volume falhou ou bem-sucedida

Você pode criar um relatório que exibe o status das transferências de volume. Pode visualizar transferências de volume falhadas e bem-sucedidas neste relatório.

### Antes de começar

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

Use as etapas a seguir para criar uma exibição personalizada para mostrar quais transferências falharam e quais foram bem-sucedidas e, em seguida, agendar um relatório a ser gerado para essa exibição.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **relacionamento > último Status da transferência de 1 meses**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que não deseja no relatório.
4. Arraste a coluna "resultado da operação" perto da coluna "Estado".
5. Clique na parte superior da coluna "resultado da operação" para classificar os volumes pelo status.
6. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo "volumes por status de transferência".
7. Clique no botão **relatórios programados** na página de inventário.
8. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados apresentados no relatório, pode investigar o estado da transferência.

## Criando um relatório para exibir transferências de volume com base no tamanho da transferência

Você pode criar um relatório para exibir transferências de volume com base no tamanho da transferência.

### Antes de começar

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

Siga as etapas a seguir para criar uma exibição personalizada para transferências de volume com base no tamanho da transferência e, em seguida, agendar um relatório a ser gerado para essa exibição.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **relacionamento > taxa de transferência de 1 meses**.
3. Clique na parte superior da coluna "Total Transfer Size" para classificar as transferências de volume por tamanho.
4. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo "volumes por tamanho de transferência".
5. Clique no botão **relatórios programados** na página de inventário.

6. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode investigar as relações de volume por tamanho de transferência.

### **Criando um relatório para exibir transferências de volume agrupadas por dia**

Você pode criar um relatório para exibir transferências de volume agrupadas por dia.

#### **Antes de começar**

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

Siga as etapas a seguir para criar uma exibição personalizada para transferências de volume agrupadas por dia e, em seguida, agendar um relatório a ser gerado para essa exibição.

#### **Passos**

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **relacionamento > taxa de transferência de 1 meses**.
3. Clique na parte superior da coluna "dia" para classificar as transferências de volume por dia.
4. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo ""Transferências de volume por dia"".
5. Clique no botão **relatórios programados** na página de inventário.
6. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode investigar as transferências de volume por dia.

### **Personalizar relatórios de desempenho de volume**

Esses relatórios personalizados de amostra são usados para ajudá-lo a identificar e responder a possíveis problemas relacionados ao desempenho de volume.

#### **Criação de um relatório para exibir volumes com uma grande quantidade de dados inativos em um agregado que não esteja habilitado para FabricPool**

Você pode criar um relatório para exibir volumes com uma grande quantidade de dados inativos em um agregado que não seja da FabricPool. Isso pode ajudar a identificar volumes que devem ser movidos para um agregado do FabricPool.

#### **Antes de começar**

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

Use as etapas a seguir para criar uma exibição personalizada para volumes com uma grande quantidade de dados inativos em um agregado não habilitado para FabricPool e, em seguida, agende um relatório a ser gerado para essa exibição.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. No menu Exibir, selecione **desempenho > todos os volumes**.
3. Selecione **Mostrar/Ocultar** para se certificar de que a coluna "tipo de disco" aparece na exibição.  
  
Adicione ou remova outras colunas para criar uma exibição importante para o relatório.
4. Arraste a coluna "Disk Type" (tipo de disco) perto da coluna "Cold Data" (dados inativos).
5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Apply Filter**:
  - Dados inativos superiores a 100 GB
  - Tipo de disco contém SSD
6. Clique na parte superior da coluna "tipo de disco" para classificar os volumes por tipo de disco, de modo que o tipo de disco SSD (FabricPool) esteja na parte inferior.
7. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo "Cold data vols not FabricPool".
8. Clique no botão **relatórios programados** na página de inventário.
9. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode encontrar volumes que são bons candidatos a serem movidos para agregados FabricPool.

## Exemplos de relatórios do Microsoft Excel

Esses relatórios de exemplo do Microsoft Excel destinam-se a introduzir opções de relatórios disponíveis usando recursos avançados do Excel.

A funcionalidade avançada do Excel pode criar uma grande variedade de relatórios específicos às suas necessidades. Para obter informações completas sobre como usar o Excel, consulte a documentação do produto.



Você deve ter a função Administrador de aplicativos ou Administrador de armazenamento para gerenciar relatórios.

### Criando um relatório para mostrar uma tabela de capacidade agregada e um gráfico

Você pode criar um relatório para analisar a capacidade em um arquivo do Excel usando totais somados e o formato de gráfico de colunas agrupadas.

#### Antes de começar

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

Use as etapas a seguir para abrir uma exibição Saúde: Todos os agregados, baixar a exibição no Excel, criar um gráfico de capacidade disponível, fazer o upload do arquivo Excel personalizado e agendar o relatório final.

### Passos

1. No painel de navegação à esquerda, clique em **Storage > Aggregates**.
2. Selecione **relatórios > Download Excel**.



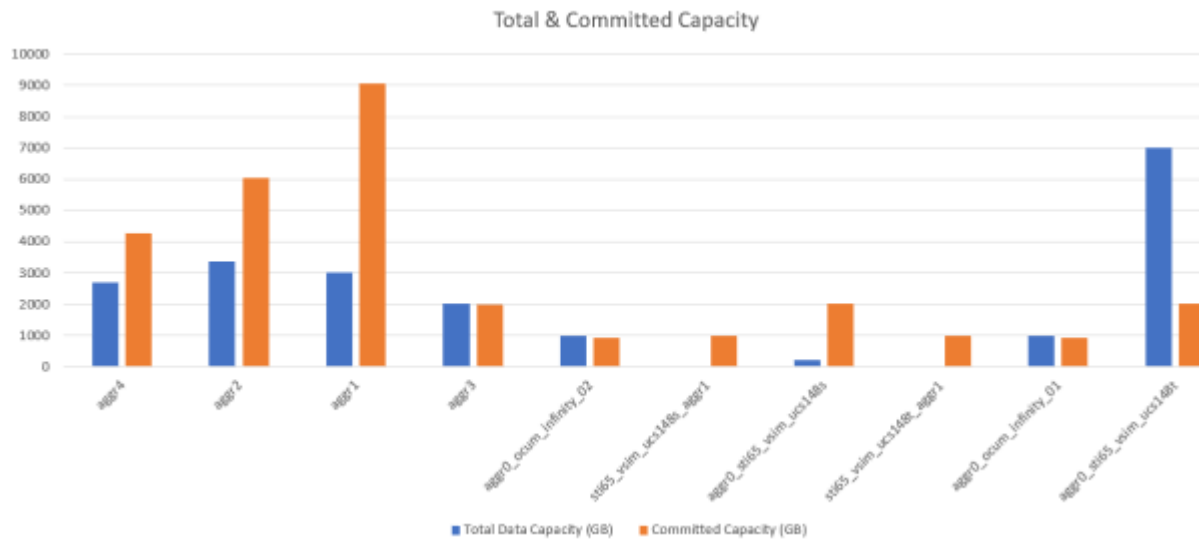
Dependendo do navegador, talvez seja necessário clicar em **OK** para salvar o arquivo.

3. Se necessário, clique em **Ativar Edição**.
4. No Excel, abra o arquivo baixado.
5. Crie uma nova folha ( **+** ) após a data folha e nomeie-a **capacidade total de dados**.
6. Adicione as seguintes colunas na nova folha capacidade total de dados:
  - a. Capacidade total de dados (GB)
  - b. Capacidade comprometida (GB)
  - c. Capacidade de dados usada (GB)
  - d. Capacidade de dados disponível (GB)
7. Na primeira linha de cada coluna, insira a seguinte fórmula, certificando-se de que ela faz referência à folha de dados (dados!), e faz referência aos especificadores de coluna e linha corretos para os dados capturados (Total Data Capacity puxa dados da coluna e, linhas 2 a 20).
  - a. (Dados!e USD 2:dados!e USD 20)
  - b. SOMA(data!F 2:data!F 50)
  - c. SOMA(data!2:data!50)
  - d. SOMA(data!H 2:data!H 50)

A fórmula totaliza cada coluna com base nos dados atuais.

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. Na folha de dados, selecione as colunas **capacidade total de dados (GB)** e **capacidade comprometida (GB)**.
2. Selecione **gráficos recomendados** no menu **Inserir** e selecione o gráfico **coluna agrupada**.
3. Clique com o botão direito do rato no gráfico e selecione **mover gráfico** para mover o gráfico para a **Total Data Capacity** folha.
4. Usando os menus **Design** e **Format**, que estão disponíveis quando o gráfico é selecionado, você pode personalizar a aparência do gráfico.
5. Quando estiver satisfeito, salve o arquivo com suas alterações. Não altere o nome ou a localização do ficheiro.



6. No Unified Manager, selecione **relatórios > carregar Excel**.



Certifique-se de que você está na mesma exibição em que você baixou o arquivo do Excel.

7. Selecione o ficheiro Excel que modificou.
8. Clique em **abrir**.
9. Clique em **Enviar**.

Uma marca de seleção aparece ao lado do item de menu **relatórios > carregar Excel**.



10. Clique em **relatórios programados**.



11. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.



Selecione o formato **XLSX** para o relatório.

12. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer investigar como usar melhor a capacidade disponível em toda a rede.

## Criando um relatório para mostrar gráficos de capacidade total agregado versus disponível

Você pode criar um relatório para analisar a capacidade total e comprometida do armazenamento em um formato de gráfico do Excel.

### Antes de começar

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

Use as etapas a seguir para abrir uma exibição Saúde: Todos os agregados, baixar a exibição no Excel, criar um gráfico de capacidade total e comprometida, fazer o upload do arquivo Excel personalizado e agendar o relatório final.

### Passos

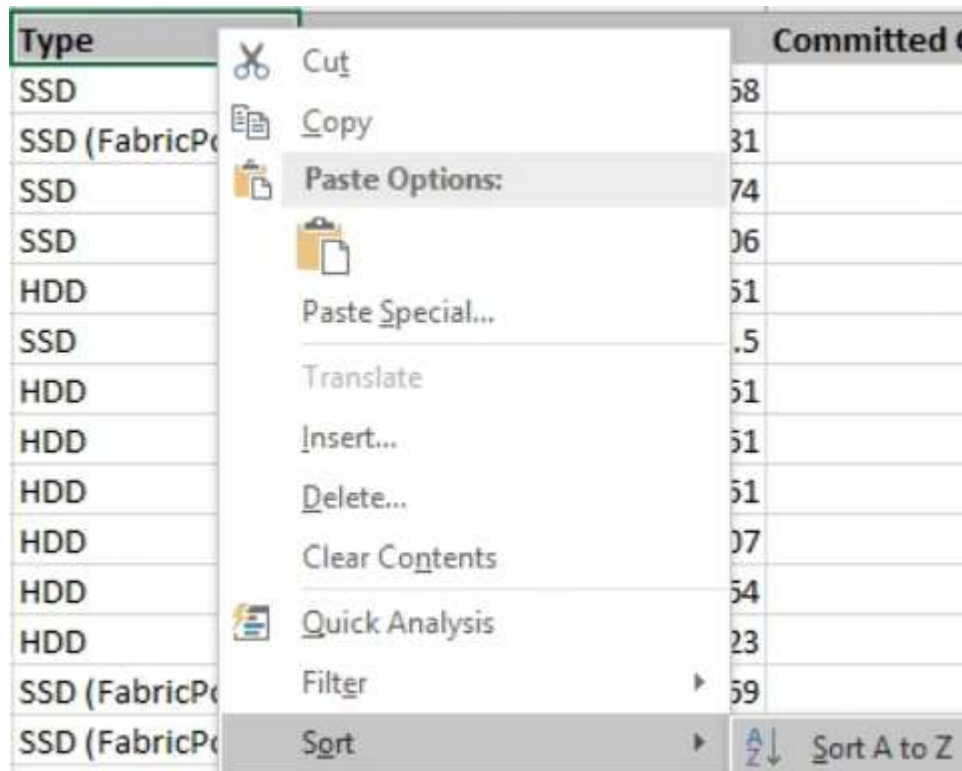
1. No painel de navegação à esquerda, clique em **Storage > Aggregates**.
2. Selecione **relatórios > Download Excel**.



Dependendo do navegador, talvez seja necessário clicar em **OK** para salvar o arquivo.

3. No Excel, abra o arquivo baixado.
4. Se necessário, clique em **Ativar Edição**.

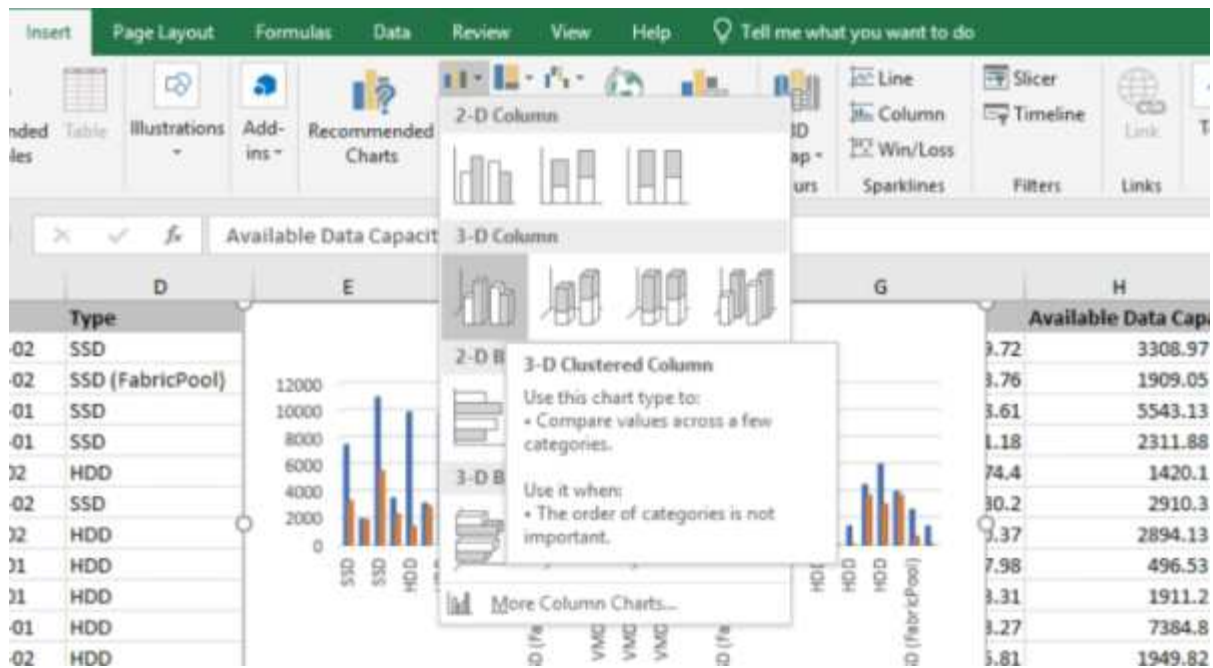
5. Na folha de dados, clique com o botão direito do rato na coluna tipo e seleccione **Ordenar > Ordenar A A Z**.



Isso organizará seus dados por tipo de armazenamento, como:

- HDD
  - Híbrida
  - SSD
  - SSD (FabricPool)
6. Seleccione **Type**, **Total Data Capacity**, as colunas e **Available Data Capacity**
7. No menu **Inserir**, seleccione um 3-D column gráfico.

O gráfico é apresentado na folha de dados.



8. Clique com o botão direito do rato no gráfico e selecione **mover Gráfico**.

9. Selecione **Nova folha** e nomeie a folha **gráficos totais de armazenamento**.

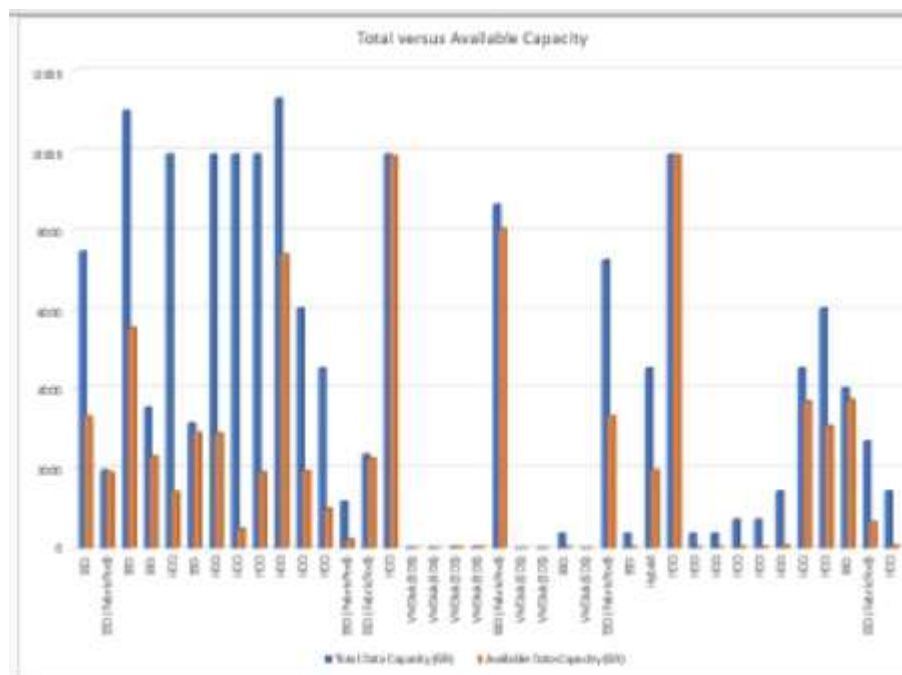


Certifique-se de que a nova folha é apresentada após as folhas de informação e dados.

10. Nomeie o título do gráfico **Total versus capacidade disponível**.

11. Usando os menus **Design** e **Format**, disponíveis quando o gráfico é selecionado, você pode personalizar a aparência do gráfico.

12. Quando estiver satisfeito, salve o arquivo com suas alterações. Não altere o nome ou a localização do ficheiro.



13. No Unified Manager, selecione **relatórios > carregar Excel**.



Certifique-se de que você está na mesma exibição em que você baixou o arquivo do Excel.

14. Selecione o ficheiro Excel que modificou.
15. Clique em **abrir**.
16. Clique em **Enviar**.

Uma marca de seleção aparece ao lado do item de menu **relatórios > carregar Excel**.

IOPS	MB/s	Utilization
1.8 IOPS	1.54 MB/s	4%
918 IOPS	43.3 MB/s	< 1%
120 IOPS	7.99 MB/s	< 1%

17. Clique em **relatórios programados**.
18. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página **Report Schedules** para que você possa definir as características de agendamento para o novo relatório.



Selecione o formato **XLSX** para o relatório.

19. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer equilibrar a carga em seus agregados.

## Criando um relatório para exibir gráficos de capacidade de volume disponíveis

Você pode criar um relatório para analisar a capacidade de volume disponível em um gráfico do Excel.

### Antes de começar

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

Siga as etapas a seguir para abrir uma exibição Saúde: Todos os volumes, baixar a exibição no Excel, criar um gráfico de capacidade disponível, fazer o upload do arquivo personalizado do Excel e agendar o relatório final.

### Passos

1. No painel de navegação esquerdo, clique em **Storage > volumes**.
2. Selecione **relatórios > Download Excel**.



Dependendo do navegador, talvez seja necessário clicar em **OK** para salvar o arquivo.

3. Se necessário, clique em **Ativar Edição**.
4. No Excel, abra o arquivo baixado.
5. Na data folha, selecione os dados que pretende utilizar nas `Volume` colunas e `Available Data %`.
6. No menu **Insert**, selecione a `3-D piechart`.

O gráfico mostra quais volumes têm o maior espaço disponível. O gráfico é apresentado na folha de dados.

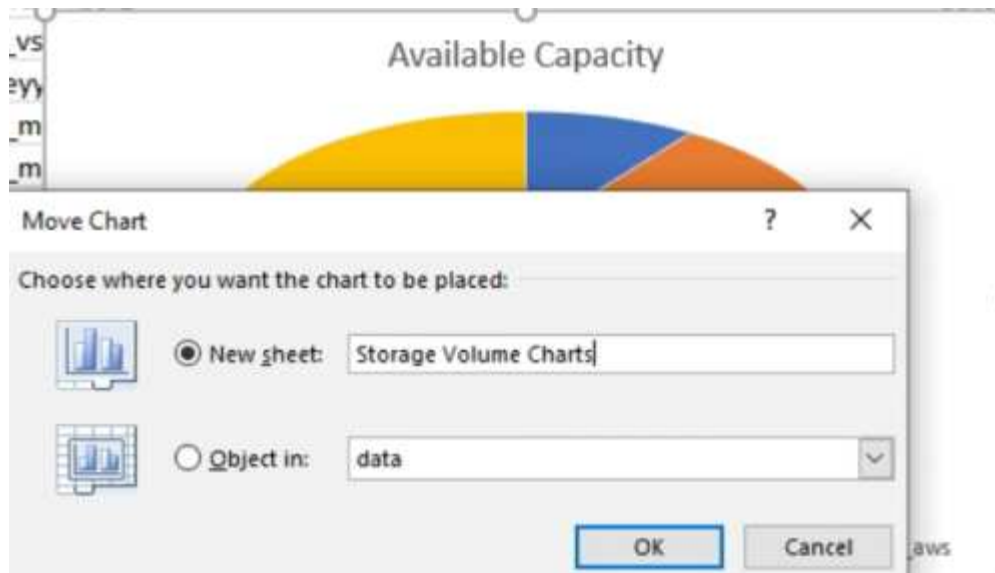


Dependendo da configuração da rede, selecionar as colunas inteiras ou muitas linhas de dados pode tornar o gráfico de pizza ilegível. Esta amostra usa o gráfico de pizza 3-D, mas você pode usar qualquer tipo de gráfico. Use o gráfico que melhor exhibe os dados que deseja capturar.

7. Nomeie o título do gráfico **capacidade disponível**.
8. Clique com o botão direito do rato no gráfico e selecione **mover Gráfico**.
9. Selecione **Nova folha** e nomeie a folha **gráficos de volume de armazenamento**.



Certifique-se de que a nova folha é apresentada após as folhas de informação e dados.



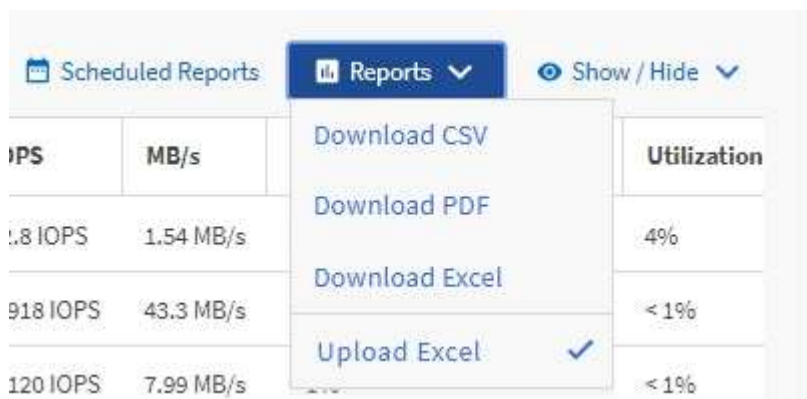
10. Usando os menus **Design** e **Format**, disponíveis quando o gráfico é selecionado, você pode personalizar a aparência do gráfico.
11. Quando estiver satisfeito, salve o arquivo com suas alterações.
12. No Unified Manager, selecione **relatórios** > **carregar Excel**.



Certifique-se de que você está na mesma exibição em que você baixou o arquivo do Excel.

13. Selecione o ficheiro Excel que modificou.
14. Clique em **abrir**.
15. Clique em **Enviar**.

Uma marca de seleção aparece ao lado do item de menu **relatórios** > **carregar Excel**.



16. Clique em **relatórios programados**.
17. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página **Report Schedules** para que você possa definir as características de agendamento para o novo relatório.
18. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.



Selecione o formato **XLSX** para o relatório.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode querer equilibrar a carga em seus volumes.

## Criação de um relatório para visualizar agregados que tenham o IOPS mais disponível

Este relatório mostra quais agregados têm o IOPS mais disponível por tipo de agregado nos quais você pode provisionar novos workloads.

### Antes de começar

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

Siga as etapas a seguir para abrir uma exibição Saúde: Todos os volumes, baixar a exibição no Excel, criar um gráfico de capacidade disponível, fazer o upload do arquivo personalizado do Excel e agendar o relatório final.

### Passos

1. No painel de navegação à esquerda, clique em **Storage > Aggregates**.
2. Selecione **desempenho: Todos os agregados** na lista suspensa **Exibir**.
3. Selecione **Mostrar/Ocultar** para mostrar a `Available IOPS` coluna e ocultar as `Cluster FQDN`, `Inactive Data Reporting`, colunas e `Threshold Policy`.
4. Arraste e largue as `Available IOPS` colunas e `Free Capacity` ao lado da `Type` coluna.
5. Nomeie e salve a exibição personalizada `Available IOPS Per Aggr`.
6. Selecione **relatórios > Download Excel**.



Dependendo do navegador, talvez seja necessário clicar em **OK** para salvar o arquivo.

7. Se necessário, clique em **Ativar Edição**.
8. No Excel, abra o arquivo baixado.
9. Na folha de dados, clique no pequeno triângulo no canto superior esquerdo da folha para selecionar a folha inteira.
10. Na faixa de opções **Data**, selecione **Classificar** no `Sort & Filter` area.

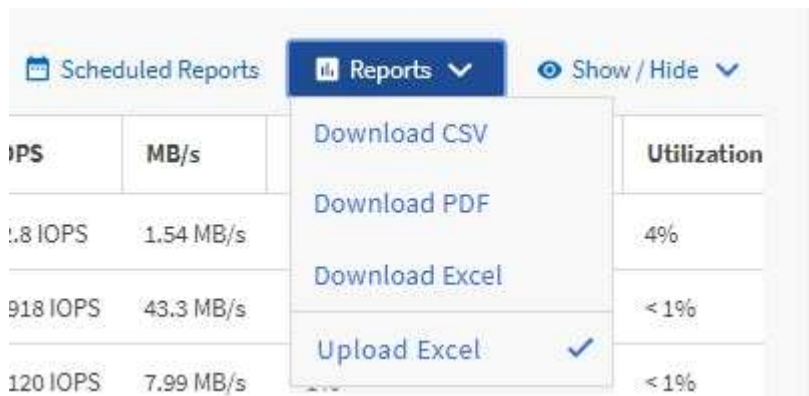
11. Defina os seguintes níveis de ordenação:
  - a. Especifique o **Ordenar por** como (IOPS), o **Ordenar por Available IOPS** como Cell Values, e o **pedido** como Largest to Smallest.
  - b. Clique em **Adicionar nível**.
  - c. Especifique o **Ordenar por** como, o **Ordenar por Type** como Cell Values, e o **pedido** como Z to A.
  - d. Clique em **Adicionar nível**.
  - e. Especifique **Ordenar por** como **Ordenar por como Ordenar por Free Capacity (GB)**, como Cell Values, e **Ordem** como Largest to Smallest.
  - f. Clique em **OK**.
12. Salve e feche o arquivo do Excel.
13. No Unified Manager, selecione **relatórios > carregar Excel**.



Certifique-se de que você está na mesma exibição em que você baixou o arquivo do Excel.

14. Selecione o ficheiro Excel que modificou, neste caso performance-aggregates-<date>.xlsx.
15. Clique em **abrir**.
16. Clique em **Enviar**.

Uma marca de seleção aparece ao lado do item de menu **relatórios > carregar Excel**.



17. Clique em **relatórios programados**.
18. Clique em **Add Schedule** (Adicionar agendamento) para adicionar uma nova linha à página Report Schedules (agendas de relatórios) para que você possa definir as características de agendamento para o novo relatório.
19. Introduza um nome para a agenda do relatório e preencha os outros campos do relatório e, em seguida, clique na marca de verificação (✓) no final da linha.



Selecione o formato **XLSX** para o relatório.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório gera e é enviado por e-mail para os destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode provisionar novos workloads nos agregados que



têm o maior IOPS disponível.

# Gerenciar o storage usando APIS REST

## Primeiros passos com as APIS REST do Active IQ Unified Manager

O Active IQ Unified Manager fornece um conjunto de APIs para gerenciar seus recursos de storage nos sistemas de storage compatíveis por meio de uma interface de serviço da Web RESTful para qualquer integração de terceiros.

Nesses tópicos, você encontrará informações sobre APIs do Unified Manager, fluxos de trabalho de exemplo para resolver problemas específicos e alguns códigos de exemplo. Usando essas informações, você pode criar clientes RESTful de soluções de software de gerenciamento NetApp para gerenciar sistemas NetApp. As APIs são baseadas no estilo arquitetônico Representational State Transfer (REST). Todas as quatro operações REST Create, Read, Update e Delete (também conhecidas como CRUD) são suportadas.

"[Active IQ Unified Manager](#)" Consulte para obter recursos adicionais e detalhes sobre os benefícios da API REST do Active IQ Unified Manager.

### Público-alvo para este conteúdo

Os tópicos aqui são destinados a desenvolvedores que criam aplicativos que fazem interface com o software Active IQ Unified Manager por meio de APIS REST.

Administradores e arquitetos de storage podem consultar essas informações para obter uma compreensão básica de como as APIs REST do Unified Manager podem ser usadas para criar aplicações clientes para gerenciar e monitorar sistemas de storage NetApp.

Use essas informações se quiser usar o provedor de storage, o cluster do ONTAP e as APIs de administração de gerenciamento para gerenciar o storage.



Você deve ter uma das seguintes funções: Operador, Administrador de armazenamento ou Administrador de aplicativos. Você deve saber o endereço IP ou o nome de domínio totalmente qualificado do servidor do Unified Manager no qual deseja executar as APIS REST.

### Acesso à API Active IQ Unified Manager e categorias

As APIs do Active IQ Unified Manager permitem que você gerencie e provisione objetos de storage em seu ambiente. Você também pode acessar a IU da Web do Unified Manager para executar algumas dessas funções.

### Construindo um URL para acessar diretamente APIs REST

Você pode acessar as REST APIs diretamente por meio de uma linguagem de programação, como Python, C, JavaScript e assim por diante. Insira o nome do host ou o endereço IP e o URL para acessar as APIS REST no formato

```
/<hostname>/api//////////
```



A porta padrão é 443. Você pode configurar a porta conforme exigido pelo seu ambiente.

## Acessando a página de documentação da API on-line

Você pode acessar a página de conteúdo de referência *Documentação da API* que é empacotada juntamente com o produto para exibir a documentação da API, bem como emitir manualmente uma chamada de API (na interface, por exemplo, Swagger). Você pode acessar esta documentação clicando em **barra de Menu > botão Ajuda > Documentação da API**

Como alternativa, insira o nome do host ou o endereço IP e o URL para acessar a página REST API no formato

```
 /<hostname>/docs/api//////////
```

## Categorias

As chamadas de API são organizadas em funcionalmente com base nas áreas ou categorias. Para localizar uma API específica, clique na categoria API aplicável.

As REST APIs fornecidas com o Unified Manager ajudam a executar funções administrativas, de monitoramento e de provisionamento. As APIs são agrupadas nas seguintes categorias.

- **data center**

Essa categoria contém as APIs que ajudam você no gerenciamento e na análise do storage de data center com ferramentas, como Work Flow Automation e Ansible. As APIs REST nesta categoria fornecem informações sobre clusters, nós, agregados, volumes, LUNs, compartilhamentos de arquivos, namespaces e outros elementos no data center.

- **servidor de gerenciamento**

As APIs sob a categoria **Management-server** contém as `jobs`, `system`, APIs e `events`. Tarefas são operações agendadas para execução assíncrona relacionadas ao gerenciamento de objetos de storage ou workloads no Unified Manager. A `events` API retorna eventos em seu data center e a `system` API retorna os detalhes da instância do Unified Manager.

- **provedor de armazenamento**

Essa categoria contém todas as APIs de provisionamento necessárias para gerenciar e provisionar compartilhamentos de arquivos, LUNs, níveis de serviço de performance e políticas de eficiência de storage. As APIs também permitem que você configure pontos de extremidade de acesso, diretórios ativos, bem como atribua níveis de Serviço de desempenho e políticas de eficiência de armazenamento em cargas de trabalho de storage.

- **administração**

Esta categoria contém as APIs usadas para executar tarefas administrativas, como manter configurações de backup, exibir certificados de armazenamento de confiança para fontes de dados do Gerenciador Unificado e gerenciar clusters do ONTAP como fontes de dados para o Gerenciador Unificado.

- **gateway**

Com o Unified Manager, você pode invocar as APIs REST do ONTAP por meio das APIs na categoria gateway e gerenciar os objetos de storage no data center.

- **segurança**

Esta categoria contém APIs para gerenciar usuários do Unified Manager.

## Serviços REST oferecidos em Active IQ Unified Manager

Você deve estar ciente dos serviços e operações REST oferecidos antes de começar a usar as APIs do Active IQ Unified Manager.

As APIs de provisionamento e administrativas usadas para configurar o servidor de API suportam as operações de leitura (GET) ou gravação (POST, PATCH, DELETE). A seguir estão alguns exemplos das operações GET, PATCH, POST e DELETE que são suportadas pelas APIs:

- Exemplo para GET: `GET /datacenter/cluster/clusters` Recupera os detalhes do cluster em seu data center. O número máximo de Registros retornados pela GET operação é 1000.



As APIs permitem filtrar, classificar e ordenar os Registros por atributos suportados.

- Exemplo para POST `POST /datacenter/svm/svms`: Cria uma máquina virtual de storage (SVM) personalizada.
- Exemplo para PATCH: `PATCH /datacenter/svm/svms/{key}` Modifica as propriedades de um SVM, usando sua chave exclusiva.
- Exemplo de EXCLUSÃO: `DELETE /storage-provider/access-endpoints/{key}` Exclui um ponto de extremidade de acesso de um LUN, SVM ou compartilhamento de arquivos usando sua chave exclusiva.

As OPERAÇÕES REST que podem ser executadas usando as APIs dependem da função do usuário Operador, Administrador de armazenamento ou Administrador de aplicativos.

Função de utilizador	Método REST suportado
Operador	Acesso somente leitura aos dados. Os usuários com essa função podem executar todas as SOLICITAÇÕES GET.
Administrador de armazenamento	Acesso de leitura a todos os dados. Os usuários com essa função podem executar todas as SOLICITAÇÕES GET.  Além disso, eles têm acesso de gravação (para executar SOLICITAÇÕES DE PATCH, POST e EXCLUSÃO) para executar atividades específicas, como gerenciamento, objetos de serviço de armazenamento e opções de gerenciamento de armazenamento.
Administrador de aplicativos	Acesso de leitura e gravação a todos os dados. Os usuários com essa função podem executar solicitações GET, PATCH, POST E DELETE para todas as funções.

Para obter mais informações sobre todas as OPERAÇÕES REST, consulte a documentação da API *Online*.

## Versão da API no Active IQ Unified Manager

As URIs da API REST no Active IQ Unified Manager especifica um número de versão. Por exemplo, `/v2/datacenter/svm/svms`. o número da versão `v2` em `/v2/datacenter/svm/svms` indica a versão da API usada em uma versão específica. O número da versão minimiza o impactos das alterações da API no software cliente, enviando de volta uma resposta que o cliente pode processar.

A parte numérica deste número de versão é incremental em relação às versões. URIs com um número de versão fornecem uma interface consistente que mantém a compatibilidade com versões anteriores em versões futuras. Você também encontra as mesmas APIs sem uma versão, por exemplo `/datacenter/svm/svms`, , que indicam as APIs base sem uma versão. As APIs base são sempre a versão mais recente das APIs.



No canto superior direito da interface do Swagger, você pode selecionar a versão da API a ser usada. A versão mais alta é selecionada por padrão. É recomendável usar a versão mais alta de uma API específica (com relação ao número inteiro incremental) disponível na instância do Unified Manager.

Para todas as solicitações, você deve solicitar explicitamente a versão da API que deseja usar. Quando o número da versão é especificado, o serviço não retorna elementos de resposta que seu aplicativo não foi projetado para lidar. Em SOLICITAÇÕES REST, você deve incluir o parâmetro versão. As versões anteriores das APIs são eventualmente obsoletas após algumas versões. Nesta versão, a `v1` versão das APIs está obsoleta.

## Recursos de storage no ONTAP

Os recursos de storage no ONTAP podem ser amplamente classificados em *recursos de storage físicos* e *recursos de storage lógicos*. para gerenciar de forma eficaz seus sistemas ONTAP usando as APIs fornecidas no Active IQ Unified Manager, você deve entender o modelo de recursos de storage e a relação entre vários recursos de storage.

- **Recursos de armazenamento físico**

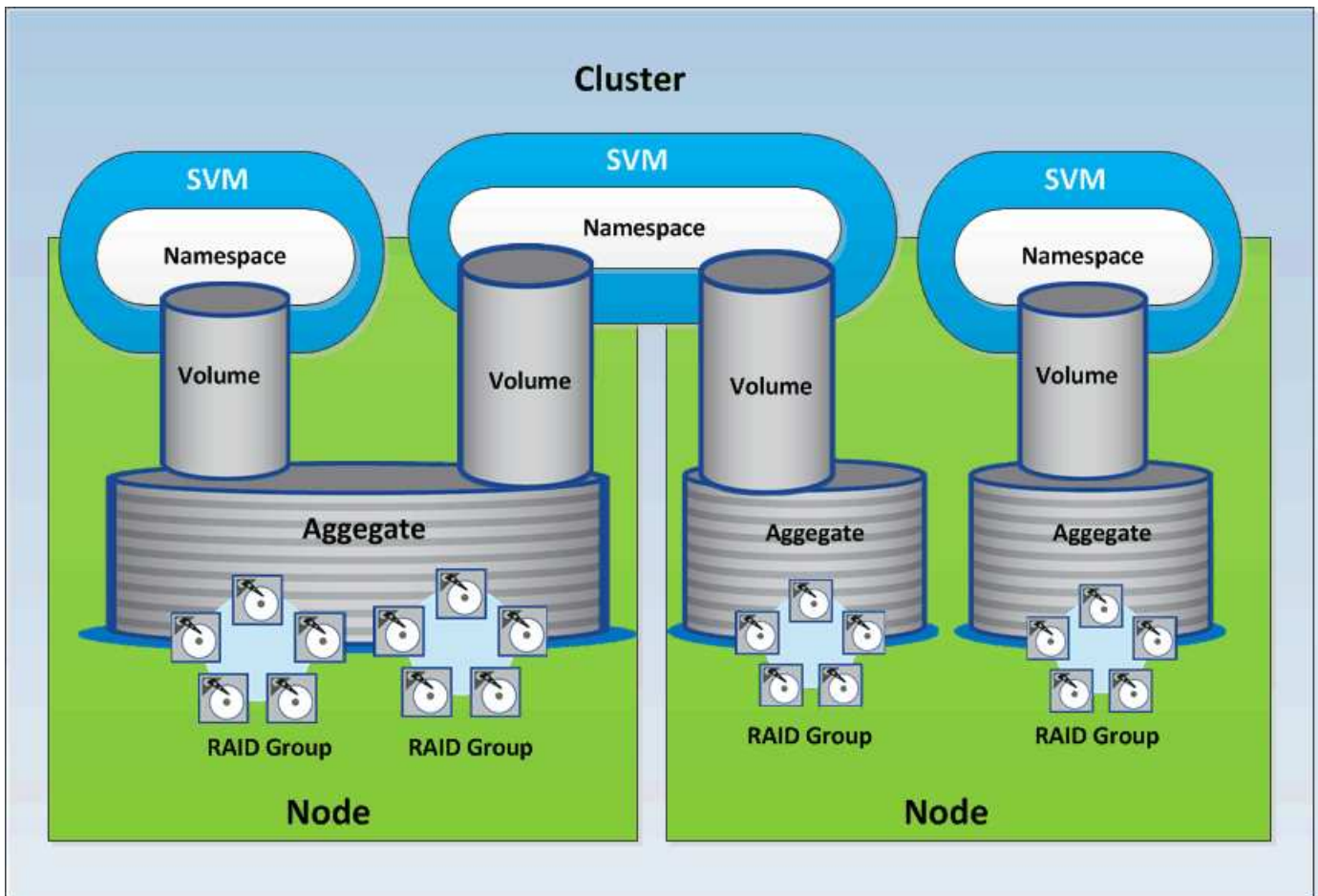
Refere-se aos objetos de armazenamento físico fornecidos pelo ONTAP. Os recursos físicos de storage incluem discos, clusters, controladores de storage, nós e agregados.

- **Recursos lógicos de armazenamento**

Refere-se aos recursos de storage fornecidos pelo ONTAP que não estão vinculados a um recurso físico. Esses recursos são associados a uma máquina virtual de storage (SVM, anteriormente conhecida como SVM) e existem independentemente de qualquer recurso de storage físico específico, como disco, LUN de array ou agregado.

Os recursos de storage lógicos incluem volumes de todos os tipos e qtrees, além dos recursos e configurações que você pode usar com esses recursos, como cópias Snapshot, deduplicação, compactação e cotas.

A ilustração a seguir mostra os recursos de armazenamento em um cluster de 2 nós:



## Acesso à API REST e autenticação no Active IQ Unified Manager

A API REST do Active IQ Unified Manager é acessível usando qualquer cliente REST ou plataforma de programação que pode emitir solicitações HTTP com um mecanismo básico de autenticação HTTP.

Uma amostra de solicitação e resposta:

- **Pedido**

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

- **Resposta**

```
{
  "records": [
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
```

```

00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
  "name": "fas8040-206-21",
  "uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
  "contact": null,
  "location": null,
  "version": {
    "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33
UTC 2019",
    "generation": 9,
    "major": 5,
    "minor": 0
  },
  "isSanOptimized": false,
  "management_ip": "10.226.207.25",
  "nodes": [
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb",
      "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
      "name": "fas8040-206-21-01",
      "_links": {
        "self": {
          "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb"
        }
      },
      "location": null,
      "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
      },
      "model": "FAS8040",
      "uptime": 13924095,
      "serial_number": "701424000157"
    },
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7",
      "uuid": "1ed606ed-2e3a-11e9-a270-00a0985bb9b7",
      "name": "fas8040-206-21-02",

```

```

    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7"
      }
    },
    "location": null,
    "version": {
      "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
      "generation": 9,
      "major": 5,
      "minor": 0
    },
    "model": "FAS8040",
    "uptime": 14012386,
    "serial_number": "701424000564"
  }
],
  "_links": {
    "self": {
      "href": "/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-
00a0985badbb"
    }
  }
},

```

- *IP address/hostname* É o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do servidor API.
- Porta 443

443 é a porta HTTPS padrão. Você pode personalizar a porta HTTPS, se necessário.

Para emitir solicitações HTTP de um navegador da Web, você precisa usar plugins de navegador REST API. Você também pode acessar a API REST usando plataformas de script como curl e Perl.

## Autenticação

O Unified Manager suporta o esquema básico de autenticação HTTP para APIs. Para um fluxo seguro de informações (solicitação e resposta), as APIS REST são acessíveis somente por HTTPS. O servidor de API fornece um certificado SSL autoassinado a todos os clientes para verificação do servidor. Este certificado pode ser substituído por um certificado personalizado (ou certificado CA).

Você deve configurar o acesso do usuário ao servidor de API para chamar as APIS REST. Os usuários podem ser usuários locais (perfis de usuário armazenados no banco de dados local) ou usuários LDAP (se você tiver configurado o servidor de API para autenticar no LDAP). Você pode gerenciar o acesso do usuário fazendo



login na interface de usuário do Unified Manager Administration Console.

## Códigos de status HTTP usados no Active IQ Unified Manager

Ao executar as APIs ou solucionar problemas, você deve estar ciente dos vários códigos de status HTTP e códigos de erro usados pelas APIs do Active IQ Unified Manager.

A tabela a seguir lista os códigos de erro relacionados à autenticação:

Código de status HTTP	Título do código de status	Descrição
200	OK	Retornado na execução bem-sucedida de chamadas de API síncronas.
201	Criado	Criação de novos recursos por chamadas síncronas, como a configuração do active Directory.
202	Aceito	Retornado na execução bem-sucedida de chamadas assíncronas para funções de provisionamento, como a criação de LUNs e compartilhamentos de arquivos.
400	Pedido inválido	Indica falha na validação da entrada. O usuário tem que corrigir as entradas, por exemplo, chaves válidas em um corpo de solicitação.
401	Solicitação não autorizada	Você não está autorizado a visualizar o recurso/não autorizado.
403	Pedido proibido	O acesso ao recurso que você estava tentando acessar é proibido.
404	Recurso não encontrado	O recurso que você está tentando acessar não foi encontrado.
405	Método não permitido	Método não permitido.
429	Demasiados pedidos	Retornado quando o usuário envia muitas solicitações dentro de um tempo específico.

Código de status HTTP	Título do código de status	Descrição
500	Erro interno do servidor	Erro interno do servidor. Falha ao obter a resposta do servidor. Este erro interno do servidor pode ou não ser permanente. Por exemplo, se executar uma GET operação ou GET ALL e receber este erro, recomenda-se que repita esta operação por um mínimo de cinco tentativas. Se for um erro permanente, o código de status retornado continuará sendo 500. Se a operação for bem-sucedida, o código de estado devolvido é 200.

## Recomendações para o uso das APIs para Active IQ Unified Manager

Ao usar as APIs no Active IQ Unified Manager, você deve seguir certas práticas recomendadas.

- Todo o tipo de conteúdo de resposta deve estar no seguinte formato para uma execução válida:

```
application/json
```

- O número da versão da API não está relacionado com o número da versão do produto. Você deve usar a versão mais recente da API disponível para sua instância do Unified Manager. Para obter mais informações sobre as versões da API do Unified Manager, consulte a seção "versão da API REST no Active IQ Unified Manager".
- Ao atualizar valores de array usando uma API do Unified Manager, você deve atualizar toda a cadeia de valores. Não é possível anexar valores a uma matriz. Você só pode substituir um array existente.
- Você pode usar operadores de filtro, como pipe (|) e Wild card para todos os parâmetros de consulta, exceto para valores duplos, por exemplo, IOPS e desempenho nas APIs de métricas.
- Evite consultar objetos usando uma combinação dos operadores de filtro Wild card e pipe (|). Ele pode recuperar um número incorreto de objetos.
- Ao usar valores para filtro, certifique-se de que o valor não contenha ? nenhum caractere. Isso é para mitigar os riscos de injeção de SQL.
- Observe que a GET solicitação (todas) para qualquer API retorna um máximo de 1000 Registros. Mesmo que você execute a consulta definindo o max\_records parâmetro para um valor maior que 1000, apenas 1000 Registros serão retornados.
- Para executar funções administrativas, é recomendável usar a IU do Unified Manager.

## Registros para resolução de problemas

Os logs do sistema permitem analisar as causas de falhas e problemas de solução de problemas que podem surgir durante a execução das APIs.

Recupere os logs do seguinte local para solucionar problemas relacionados às chamadas de API.

Localização do registro	Utilização
<code>/var/log/ocie/access_log.log</code>	<p>Contém todos os detalhes da chamada da API, como o nome de usuário do usuário que invoca a API, hora de início, hora de execução, status e URL.</p> <p>Você pode usar esse arquivo de log para verificar as APIs usadas com frequência ou solucionar problemas de qualquer fluxo de trabalho de GUI. Você também pode usá-lo para dimensionar a análise, com base no tempo de execução.</p>
<code>/var/log/ocum/ocumserver.log</code>	<p>Contém todos os logs de execução da API.</p> <p>Você pode usar esse arquivo de log para solucionar problemas e depurar as chamadas de API.</p>
<code>/var/log/ocie/server.log</code>	<p>Contém todas as implantações de servidor Wildfly e logs relacionados ao serviço de início/parada.</p> <p>Você pode usar esse arquivo de log para encontrar a causa raiz de qualquer problema que ocorra durante o início, parada ou implantação do servidor Wildfly.</p>
<code>/var/log/ocie/au.log</code>	<p>Contém registros relacionados com a unidade de aquisição.</p> <p>Você pode usar esse arquivo de log quando criar, modificar ou excluir quaisquer objetos no ONTAP, mas eles não são refletidos nas APIs REST do Active IQ Unified Manager.</p>

## Objetos de trabalho processos assíncronos

O Active IQ Unified Manager fornece a `jobs` API que recupera informações sobre as tarefas executadas durante a execução de outras APIs. Você deve saber como o processamento assíncrono funciona usando o objeto trabalho.

Algumas das chamadas de API, particularmente aquelas usadas para adicionar ou modificar recursos, podem levar mais tempo para serem concluídas do que outras chamadas. O Unified Manager processa essas solicitações de longa execução assincronamente.

### Solicitações assíncronas descritas usando o objeto Job

Depois de fazer uma chamada de API que é executada de forma assíncrona, o código de resposta HTTP 202 indica que a solicitação foi validada e aceita com sucesso, mas ainda não foi concluída. A solicitação é processada como uma tarefa em segundo plano que continua a ser executada após a resposta HTTP inicial ao cliente. A resposta inclui o objeto Job ancorando a solicitação, incluindo seu identificador exclusivo.

## Consultando o objeto Job associado a uma solicitação de API

O objeto Job retornado na resposta HTTP contém várias propriedades. Você pode consultar a propriedade State para determinar se a solicitação foi concluída com sucesso. Um objeto Job pode estar num dos seguintes estados:

- NORMAL
- WARNING
- PARTIAL\_FAILURES
- ERROR

Há duas técnicas que você pode usar ao fazer polling de um objeto Job para detetar um estado terminal para a tarefa, seja com sucesso ou falha:

- Solicitação padrão de polling: O estado atual da tarefa é retornado imediatamente.
- Solicitação de polling longa: Quando o estado da tarefa se move para NORMAL, ERROR, ou PARTIAL\_FAILURES.

## Etapas em uma solicitação assíncrona

Você pode usar o seguinte procedimento de alto nível para concluir uma chamada assíncrona de API:

1. Emita a chamada assíncrona da API.
2. Receber uma resposta HTTP 202 indicando aceitação bem-sucedida da solicitação.
3. Extraia o identificador do objeto Job do corpo de resposta.
4. Dentro de um loop, aguarde que o objeto Job atinja o estado terminal NORMAL, ERROR, ou PARTIAL\_FAILURES.
5. Verifique o estado do terminal do trabalho e recupere o resultado do trabalho.

## Olá servidor API

O *Hello API Server* é um programa de exemplo que demonstra como invocar uma API REST no Active IQ Unified Manager usando um cliente REST simples. O programa de exemplo fornece detalhes básicos sobre o servidor de API no formato JSON (o servidor suporta apenas `application/json` o formato).

O URI usado é: <https://<hostname>/api/datacenter/svm/svms>. Este código de amostra toma os seguintes parâmetros de entrada:

- O endereço IP do servidor API ou FQDN
- Opcional: Número da porta (padrão: 443)
- Nome de utilizador
- Palavra-passe
- Formato da resposta (`application/json`)

Para invocar APIs REST, você também pode usar outros scripts como Jersey e RESTEasy para escrever um cliente REST Java para Active IQ Unified Manager. Você deve estar ciente das seguintes considerações sobre

o código de exemplo:

- Usa uma conexão HTTPS com o Active IQ Unified Manager para invocar o URI REST especificado
- Ignora o certificado fornecido pelo Active IQ Unified Manager
- Ignora a verificação do nome do host durante o handshake
- Utiliza `javax.net.ssl.HttpURLConnection` para uma ligação URI
- Usa uma biblioteca de (`org.apache.commons.codec.binary.Base64` terceiros ) para construir a cadeia de caracteres codificada Base64 usada na autenticação básica HTTP

Para compilar e executar o código de exemplo, você deve usar o compilador Java 1,8 ou posterior.

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
    necessary steps
     * to invoke the REST URI and show the response
    */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
            System.exit(1);
        }
        setUserArguments(args);
        String serverBaseUrl = "https://" + server;
        if (null != port) {
            serverBaseUrl = serverBaseUrl + ":" + port;
        }
    }
}
```

```

    }
    server_url = serverBaseUrl + "/api/datacenter/svm/svms";
    try {
        HttpURLConnection connection =
getAllTrustingHttpsURLConnection();
        if (connection == null) {
            System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
            System.exit(1);
        }
        System.out.println("Invoking API: " + server_url);
        connection.setRequestMethod("GET");
        connection.setRequestProperty("Accept", "application/" +
response_format);
        String authString = getAuthorizationString();
        connection.setRequestProperty("Authorization", "Basic " +
authString);
        if (connection.getResponseCode() != 200) {
            System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
                + connection.getResponseMessage());
            System.exit(1);
        }
        BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
        String response;
        System.out.println("Response:");
        while ((response = br.readLine()) != null) {
            System.out.println(response);
        }
        connection.disconnect();
    } catch (Exception e) {
        e.printStackTrace();
    }
}

/* Print the usage of this sample code */ private static void
printUsage() {
    System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
    System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
    System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
    System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
}

```

```

        System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
        System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
    }

    /* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
        String[] args) {
        server = args[0];
        user = args[1];
        password = args[2];
        if (server.contains(":")) {
            String[] parts = server.split(":");
            server = parts[0];
            port = parts[1];
        }
    }

    /*
    * * Create a trust manager which accepts all certificates and * use
this trust
    * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
    * SSL Context and skip * server hostname verification during SSL
handshake. * *
    * Note: Trusting all certificates or skipping hostname verification *
is not
    * required for API Services to work. These are done here to * keep
this sample
    * REST Client code as simple as possible.
    */ private static HttpURLConnection
getAllTrustingHttpsURLConnection() {
    HttpURLConnection conn =
    null;
    try {
        /* Creating a trust manager that does not
validate certificate chains */
        TrustManager[]
trustAllCertificatesManager = new
        TrustManager[]{new
X509TrustManager() {
            public X509Certificate[] getAcceptedIssuers(){return null;}
            public void checkClientTrusted(X509Certificate[]
certs, String authType){}
            public void checkServerTrusted(X509Certificate[]
certs, String authType){}
        }};
        /* Initialize the
SSLContext with the all-trusting trust manager */
        SSLContext sslContext = SSLContext.getInstance("TLS");
        sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
    }
}

```

```

HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));          URL url = new URL(server_url);          conn =
(HttpsURLConnection) url.openConnection();          /* Do not perform an
actual hostname verification during SSL Handshake.          Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {          public
boolean verify(String host, SSLSession          session) {
return true;          }          });          } catch (Exception e)
{          e.printStackTrace();          }          return conn;          }

/*
 * * This forms the Base64 encoded string using the username and
password *
 * provided by the user. This is required for HTTP Basic
Authentication.
 */ private static String getAuthorizationString() {
String userPassword = user + ":" + password;
byte[] authEncodedBytes =
Base64.encodeBase64(userPassword.getBytes());
String authString = new String(authEncodedBytes);
return authString;
}
}

```

## APIs REST do Unified Manager

As APIs REST para Active IQ Unified Manager estão listadas nesta seção, com base em suas categorias.

Você pode exibir a página de documentação on-line da instância do Unified Manager que inclui os detalhes de cada chamada de API REST. Este documento não repete os detalhes da documentação online. Cada chamada de API listada ou descrita neste documento inclui apenas as informações necessárias para localizar a chamada na página de documentação. Depois de localizar uma chamada de API específica, você pode revisar os detalhes completos dessa chamada, incluindo os parâmetros de entrada, formatos de saída, códigos de status HTTP e tipo de processamento de solicitação.

As seguintes informações são incluídas para cada chamada de API dentro de um fluxo de trabalho para ajudar a localizar a chamada na página de documentação:

- Categoria

As chamadas de API são organizadas na página de documentação em áreas ou categorias relacionadas à funcionalidade. Para localizar uma chamada de API específica, role para baixo até a parte inferior da página e clique na categoria de API aplicável.

- HTTP verb (chamada)

O verbo HTTP identifica a ação executada em um recurso. Cada chamada de API é executada através de



um único verbo HTTP.

- Caminho

O caminho determina o recurso específico para o qual a ação usa como parte da execução de uma chamada. A cadeia de caracteres do caminho é anexada ao URL principal para formar a URL completa que identifica o recurso.

## Gerenciamento de objetos de storage em um data center usando APIs

As APIs REST `datacenter` na categoria permitem gerenciar objetos de storage em seu data center, como clusters, nós, agregados, VMs de storage, volumes, LUNs, compartilhamentos de arquivos e namespaces. Essas APIs estão disponíveis para consultar a configuração dos objetos, enquanto algumas delas permitem que você execute as operações de adição, exclusão ou modificação desses objetos.

A maioria dessas APIs são chamadas que fornecem agregação entre clusters com suporte a filtragem, classificação e paginação. Ao executar essas APIs, elas retornam dados do banco de dados. Portanto, os recém-criados-objetos precisam ser descobertos pelo próximo ciclo de aquisição para aparecer na resposta.

Se você quiser consultar os detalhes de um objeto específico, você precisa inserir o ID exclusivo desse objeto para visualizar seus detalhes. Por exemplo, para obter informações sobre métricas e análises dos objetos de storage, "[Visualização de métricas de desempenho](#)" consulte .

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```



Os comandos CURL, exemplos, solicitações e respostas às APIs estão disponíveis na interface da API Swagger. Você pode filtrar e encomendar os resultados por parâmetros específicos, como indicado no Swagger. Essas APIs permitem filtrar os resultados para objetos de storage específicos, como cluster, volume ou VM de storage.

### APIs para objetos de storage em seu data center

Verbo HTTP	Caminho	Descrição
GET	<code>/datacenter/cluster/clusters</code>  <code>/datacenter/cluster/clusters/{key}</code>	Use esse método para visualizar os detalhes dos clusters do ONTAP no data center. A API retorna informações, como o endereço IPv4 ou IPv6 do cluster, informações sobre o nó, como integridade do nó, capacidade de desempenho e par de alta disponibilidade (HA), e indica se o cluster é All SAN Array.

Verbo HTTP	Caminho	Descrição
GET	<pre>/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}</pre>	Retorna os detalhes das licenças instaladas nos clusters do seu data center. Você pode filtrar seus resultados com base nos critérios necessários. Informações, como a chave de licença, a chave do cluster, a data de expiração e o escopo da licença são retornadas. Você pode inserir uma chave de licença para recuperar os detalhes de uma licença específica.
GET	<pre>/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}</pre>	Você pode usar esse método para exibir os detalhes dos nós no data center. É possível exibir informações sobre o cluster, a integridade do nó, a capacidade de performance e o par de alta disponibilidade (HA) para o nó.
GET	<pre>/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}</pre>	Você pode usar esse método para visualizar os detalhes dos compartilhamentos CIFS no data center. Além dos detalhes do cluster, SVM e volume, as informações sobre a ACL (Access Control List) também são retornadas.
GET	<pre>/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}</pre>	<p>Você pode usar esse método para exibir os detalhes das políticas de exportação dos serviços NFS compatíveis.</p> <p>Você pode consultar as políticas de exportação de um cluster ou VM de storage e reutilizar a chave de política de exportação para provisionar compartilhamentos de arquivos NFS. Para obter mais informações sobre a atribuição e a reutilização de políticas de exportação em workloads, consulte "Aprovisionamento de compartilhamentos de arquivos CIFS e NFS".</p>

<b>Verbo HTTP</b>	<b>Caminho</b>	<b>Descrição</b>
GET	/datacenter/storage/aggregates  /datacenter/storage/aggregates/{key}	Use esse método para visualizar a coleção de agregados no data center ou um agregado específico para provisionar workloads ou monitorar. As informações, como detalhes de cluster e nó, capacidade de performance usada, espaço disponível e usado, e eficiência de storage, são retornadas.
GET	/datacenter/storage/luns  /datacenter/storage/luns/{key}	Você pode usar esse método para exibir a coleta de LUNs em todo o data center. Você pode exibir informações sobre o LUN, como detalhes do cluster e SVM, políticas de QoS e grupos de pessoas.
GET	/datacenter/storage/qos/policies  /datacenter/storage/qos/policies/{key}	Você pode usar esse método para exibir os detalhes de todas as políticas de QoS aplicáveis aos objetos de storage no data center. As informações, como os detalhes do cluster e do SVM, os detalhes da política fixa ou adaptável e o número de objetos aplicáveis a essa política, são retornadas.
GET	/datacenter/storage/qtrees  /datacenter/storage/qtrees/{key}	Use esse método para visualizar os detalhes de qtree no data center de todos os volumes do FlexVol ou volumes do FlexGroup. Informações, como os detalhes do cluster e da SVM, FlexVol volume e política de exportação, são retornadas.

Verbo HTTP	Caminho	Descrição
GET	/datacenter/storage/volumes  /datacenter/storage/volumes/{key}	<p>Você pode usar esse método para exibir a coleta de volumes no data center. Informações sobre os volumes, como SVM e detalhes de cluster, QoS e políticas de exportação, independentemente de o volume ser do tipo leitura-gravação, proteção de dados ou compartilhamento de carga, são retornadas.</p> <p>Para volumes FlexVol e FlexClone, é possível visualizar as informações sobre os respectivos agregados. Para um volume FlexGroup, a consulta retorna a lista de agregados constituintes.</p>

Verbo HTTP	Caminho	Descrição
GET POST DELETE PATCH	/datacenter/protocols/san/ igroups  /datacenter/protocols/san/ igroups/{key}	<p>Você pode atribuir grupos de iniciadores (grupos de iniciadores) autorizados a acessar determinados destinos de LUN. Se houver um grupo existente, você pode atribuí-lo. Você também pode criar grupos e atribuí-los aos LUNs.</p> <p>Você pode usar esses métodos para consultar, criar, excluir e modificar grupos, respectivamente.</p> <p>Pontos a observar:</p> <ul style="list-style-type: none"> <li>• <b>POST</b>: Ao criar um grupo, você pode designar a VM de armazenamento na qual deseja atribuir acesso.</li> <li>• <b>DELETE</b>: Você precisa fornecer a chave do grupo como um parâmetro de entrada para excluir um determinado grupo. Se você já tiver atribuído um grupo a um LUN, não poderá excluir esse grupo.</li> <li>• <b>PATCH</b>: Você precisa fornecer a chave do grupo como um parâmetro de entrada para modificar um determinado grupo. Você também deve inserir a propriedade que deseja atualizar, juntamente com seu valor.</li> </ul>

Verbo HTTP	Caminho	Descrição
GET	/datacenter/svm/svms	<p>Você pode usar esses métodos para exibir, criar, excluir e modificar máquinas virtuais de armazenamento (VMs de armazenamento).</p> <ul style="list-style-type: none"> <li>• <b>POST</b>: Você deve inserir o objeto de VM de storage que deseja criar como parâmetro de entrada. Você pode criar uma VM de armazenamento personalizada e, em seguida, atribuir as propriedades necessárias a ela.</li> <li>• <b>DELETE</b>: Você precisa fornecer a chave de VM de armazenamento para excluir uma VM de armazenamento específica.</li> <li>• <b>PATCH</b>: Você precisa fornecer a chave de VM de storage para modificar uma VM de storage específica. Você também precisa inserir as propriedades que deseja atualizar, juntamente com seus valores.</li> </ul>
POST	/datacenter/svm/svms/{key}	
DELETE		
PATCH		



#### Pontos a observar:

Se você tiver ativado o provisionamento de workload baseado em SLO no seu ambiente enquanto cria a VM de storage, garanta que ela seja compatível com todos os protocolos necessários para provisionamento de LUNs e compartilhamentos de arquivos neles, por exemplo, CIFS ou SMB, NFS, FCP e iSCSI. Os fluxos de trabalho de provisionamento podem falhar se a VM de storage não oferecer suporte aos serviços necessários. Recomenda-se que os serviços para os respectivos tipos de cargas de trabalho também estejam ativados na VM de storage.

Se você ativou o provisionamento de workload baseado em SLO no seu ambiente, não poderá excluir essa VM de storage na qual as cargas de trabalho de storage foram provisionadas. Quando você exclui uma VM de armazenamento em que um servidor CIFS ou SMB foi configurado, essa API também exclui o servidor CIFS ou SMB, juntamente com a configuração local do ative Directory. No entanto, o nome do servidor CIFS ou SMB continua na configuração do ative Directory que você deve excluir manualmente do servidor do ative Directory.

### APIs para elementos de rede em seu data center

As seguintes APIs na categoria de data center recuperam informações sobre as portas e interfaces de rede em seu ambiente, especificamente as portas FC, interfaces FC, portas ethernet e interfaces IP.

Verbo HTTP	Caminho	Descrição
GET	<pre>/datacenter/network/ethernet/ports</pre> <pre>/datacenter/network/ethernet/ports/{key}</pre>	Recupera informações sobre todas as portas ethernet em seu ambiente de data center. Com uma chave de porta como parâmetro de entrada, você pode exibir as informações dessa porta específica. As informações, como detalhes do cluster, domínio de broadcast, detalhes da porta, como estado, velocidade e tipo, e se a porta está ativada, são recuperadas.
GET	<pre>/datacenter/network/fc/interfaces</pre> <pre>/datacenter/network/fc/interfaces/{key}</pre>	Use esse método para visualizar os detalhes das interfaces FC no ambiente de data center. Com uma chave de interface como parâmetro de entrada, você pode visualizar as informações dessa interface específica. As informações, como detalhes do cluster, detalhes do nó inicial e detalhes da porta inicial, são recuperadas.
GET	<pre>/datacenter/network/fc/ports</pre> <pre>/datacenter/network/fc/ports/{key}</pre>	Recupera informações sobre todas as portas FC usadas nos nós do ambiente do data center. Com uma chave de porta como parâmetro de entrada, você pode exibir as informações dessa porta específica. Informações, como detalhes do cluster, descrição da porta, protocolo suportado e o estado da porta são recuperadas.
GET	<pre>/datacenter/network/ip/interfaces</pre> <pre>/datacenter/network/ip/interfaces/{key}</pre>	Você pode usar esse método para exibir os detalhes das interfaces IP em seu ambiente de data center. Com uma chave de interface como parâmetro de entrada, você pode visualizar as informações dessa interface específica. As informações, como detalhes do cluster, detalhes do espaço IP, detalhes do nó inicial, se o failover está ativado, são recuperadas.

## Acessando APIs do ONTAP por meio de acesso proxy

As APIs de gateway oferecem a vantagem de usar as credenciais Active IQ Unified


Manager para executar APIs REST do ONTAP e gerenciar objetos de storage. Essas APIs estão disponíveis quando o recurso API Gateway está habilitado na IU da Web do Unified Manager.

As APIs REST do Unified Manager suportam apenas um conjunto seletivo de ações a serem executadas nos datasources do Unified Manager, ou seja, clusters do ONTAP. Você pode aproveitar os outros recursos por meio das APIs do ONTAP. As APIs de gateway permitem que o Unified Manager seja uma interface de passagem para tunelamento de todas as solicitações de API a serem executadas em clusters do ONTAP que ele gerencia, sem fazer login em cada cluster de data center individualmente. Ele funciona como um ponto único de gerenciamento para executar as APIs nos clusters do ONTAP gerenciados pela sua instância do Unified Manager. O recurso API Gateway permite que o Unified Manager seja um único plano de controle a partir do qual você pode gerenciar vários clusters ONTAP, sem fazer login neles individualmente. As APIs de gateway permitem que você permaneça conectado ao Unified Manager e gerencie os clusters do ONTAP executando operações de API REST do ONTAP.




Todos os usuários podem executar uma consulta usando a operação GET. Os administradores de aplicativos podem executar todas as operações REST do ONTAP.

O gateway atua como um proxy para túnel as solicitações de API, mantendo as solicitações de cabeçalho e corpo no mesmo formato que nas APIs do ONTAP. Você pode usar suas credenciais do Unified Manager e executar operações específicas para acessar e gerenciar os clusters do ONTAP sem passar credenciais de cluster individuais. Ele continua a gerenciar a autenticação de cluster e o gerenciamento de cluster, mas redireciona as solicitações de API para serem executadas diretamente no cluster específico. A resposta retornada pelas APIs é a mesma que a resposta retornada pelas respectivas APIs REST do ONTAP executadas diretamente do ONTAP.

Verbo HTTP	Caminho (URL)	Descrição
GET	/gateways	<p>Esse MÉTODO GET recupera a lista de todos os clusters gerenciados pelo Gerenciador Unificado que oferecem suporte a chamadas REST do ONTAP. Você pode verificar os detalhes do cluster e optar por executar outros métodos com base no UUID do cluster ou identificador exclusivo universal (UUID).</p> <p> As APIs de gateway recuperam apenas os clusters com suporte do ONTAP 9.5 ou posterior e são adicionados ao Unified Manager em HTTPS.</p>



Verbo HTTP	Caminho (URL)	Descrição
GET POST DELETE PATCH OPTIONS (Não disponível na Swagger) HEAD (Não disponível na Swagger)	/gateways/{uuid}/{path} <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-left: 20px;">  <p>O valor de uuid tem de ser substituído pelo UUID de cluster no qual a operação DE DESCANSO deve ser executada. Além disso, certifique-se de que o UUID seja do cluster compatível com o ONTAP 9.5 ou posterior e adicionado ao Unified Manager em HTTPS. O caminho deve ser substituído pelo URL REST do ONTAP. Você deve remover /api/ do URL.</p> </div>	<p>Esta é uma API proxy de ponto único, suportando operações POST, DELETE, PATCH e GET para todas as APIs REST do ONTAP. Nenhuma restrição se aplica a qualquer API, desde que seja suportada pelo ONTAP. A funcionalidade de tunelamento ou proxy não pode ser desativada.</p> <p>O OPTIONS método retorna todas as operações suportadas por uma API REST do ONTAP. Por exemplo, se uma API ONTAP suporta apenas a GET operação, executar o OPTIONS método usando esta API de gateway retorna GET como a resposta. Este método não é suportado no Swagger, mas pode ser executado em outras ferramentas de API.</p> <p>O OPTIONS método determina se um recurso está disponível. Esta operação pode ser usada para visualizar os metadados sobre um recurso nos cabeçalhos de resposta HTTP. Este método não é suportado no Swagger, mas pode ser executado em outras ferramentas de API.</p>

## Entendendo o encapsulamento do API Gateway

As APIs de gateway permitem gerenciar objetos do ONTAP por meio do Gerenciador Unificado. O Unified Manager gerencia os clusters e os detalhes de autenticação e redireciona as solicitações para o endpoint REST do ONTAP. A API de gateway transforma a URL e a Hypermedia como o mecanismo de Estado da aplicação (HATEOAS) links no cabeçalho e corpo de resposta com a URL base do gateway API. A API do gateway atua como o URL base do proxy ao qual você adiciona o URL REST do ONTAP e executa o endpoint REST do ONTAP necessário.



Para que uma API do ONTAP seja executada com sucesso por meio do gateway da API, a API deve ser suportada por essa versão do cluster do ONTAP no qual está sendo executada. Executar uma API que não é suportada no cluster ONTAP não retorna resultados.

Neste exemplo, a API de gateway (URL base proxy) é: /gateways/{uuid}/

A API ONTAP tomada é: /storage/volumes. Você precisa adicionar o URL REST da API do ONTAP como o valor para o parâmetro path.



Ao adicionar o caminho, certifique-se de que você removeu o "/" symbol at the beginning of the URL. For the API `/storage/volumes`, add `storage/volumes`.

O URL anexado é: `/gateways/{uuid}/storage/volumes`

Ao executar a GET operação, o URL gerado é o seguinte:

```
GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes
```

A `/api` tag da URL REST do ONTAP é removida no URL anexado e essa para a API do gateway é mantida.

- Sample curl comando\*

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

A API retorna a lista de volumes de armazenamento nesse cluster. O formato de resposta é o mesmo que você recebe quando executa a mesma API do ONTAP. Os códigos de status retornados são os códigos de status REST do ONTAP.

### Configurando o escopo da API

Todas as APIs têm um contexto definido dentro do escopo do cluster. As APIs que operam com base nas VMs de storage também têm o cluster como escopo, ou seja, as operações de API são executadas em uma VM de storage específica em um cluster gerenciado. Ao executar a `/gateways/{uuid}/{path}` API, certifique-se de inserir o cluster UUID (Unified Manager datasource UUID) para o cluster no qual você executa a operação. Para definir o contexto para uma VM de armazenamento específica dentro desse cluster, insira a chave VM de armazenamento como o parâmetro `X-Dot-SVM-UUID` ou o nome da VM de armazenamento como o parâmetro `X-Dot-SVM-Name`. O parâmetro é adicionado como o filtro no cabeçalho da cadeia de caracteres e a operação é executada dentro do escopo dessa VM de armazenamento dentro desse cluster.

- Sample curl comando\*

```
curl -X GET "https://<hostname>/api/gateways/e4f33f90-f75f-11e8-9ed9-00a098e3215f/storage/volume" -H "accept: application/hal+json" -H "X-Dot-SVM-UUID: d9c33ec0-5b61-11e9-8760-00a098e3215f" -H "Authorization: Basic <Base64EncodedCredentials>"
```

Para obter mais informações sobre como usar APIS REST do ONTAP, consulte ["Automação da API REST do ONTAP"](#)

### Executar tarefas administrativas usando APIs

Você pode usar as APIs `administration` na categoria para modificar configurações de backup, verificar as informações do arquivo de backup e certificados de cluster e também gerenciar clusters do ONTAP como fontes de dados do Active IQ Unified Manager.



Você deve ter a função Administrador do aplicativo para executar essas operações. Você também pode usar a IU da Web do Unified Manager para configurar essas configurações.

Verbo HTTP	Caminho	Descrição
GET PATCH	/admin/backup-settings	<p>Você pode usar o GET método para exibir as configurações do agendamento de backup configurado no Unified Manager por padrão. Você pode verificar o seguinte:</p> <ul style="list-style-type: none"><li>• Se a programação está ativada ou desativada</li><li>• Frequência da cópia de segurança agendada (diária ou semanal)</li><li>• Hora do backup</li><li>• Número máximo de arquivos de backup que devem ser mantidos no aplicativo</li></ul> <p>A hora do backup está no fuso horário do servidor.</p> <p>As configurações de backup do banco de dados estão disponíveis no Unified Manager por padrão e você não pode criar um agendamento de backup. No entanto, você pode usar o PATCH método para modificar as configurações padrão.</p>
GET	/admin/backup-file-info	<p>Um arquivo de despejo de backup é gerado sempre que o agendamento de backup é modificado para o Unified Manager. Pode utilizar este método para verificar se o ficheiro de cópia de segurança é gerado de acordo com as definições de cópia de segurança modificadas e se as informações no ficheiro correspondem às definições modificadas.</p>

Verbo HTTP	Caminho	Descrição
GET	/admin/datasource-certificate	Você pode usar este método para exibir o certificado da fonte de dados (cluster) do armazenamento de confiança. A validação do certificado é necessária antes de adicionar um cluster do ONTAP como uma fonte de dados do Unified Manager.
GET POST PATCH DELETE	/admin/datasources/cluster s  /admin/datasources/cluster s/{key}	Você pode usar o GET método para recuperar os detalhes das fontes de dados (clusters do ONTAP) gerenciadas pelo Unified Manager.  Você também pode adicionar um novo cluster ao Unified Manager como uma fonte de dados. Para adicionar um cluster, você deve saber seu nome de host, nome de usuário e senha.  Para modificar e excluir um cluster gerenciado como uma fonte de dados pelo Unified Manager, use a chave de cluster do ONTAP.

## Gerenciamento de usuários usando APIs

Você pode usar as APIs *security* na categoria para controlar o acesso do usuário a objetos de cluster selecionados no Active IQ Unified Manager. Você pode adicionar usuários locais ou usuários de banco de dados. Você também pode adicionar usuários remotos ou grupos que pertencem a um servidor de autenticação. Com base no Privileges das funções atribuídas aos usuários, eles podem gerenciar os objetos de storage ou exibir os dados no Unified Manager.



Você deve ter a função Administrador do aplicativo para executar essas operações. Você também pode usar a IU da Web do Unified Manager para configurar essas configurações.

As APIs sob a *security* categoria usam o parâmetro *usuários*, que é o nome do usuário, e não o parâmetro *chave* como o identificador exclusivo para a entidade do usuário.

Verbo HTTP	Caminho	Descrição
GET POST	/security/users	Você pode usar esses métodos para obter os detalhes dos usuários ou adicionar novo usuário ao Unified Manager.  Você pode adicionar funções específicas aos usuários com base em seus tipos de usuário. Ao adicionar usuários, você deve fornecer senhas para o usuário local, usuário de manutenção e usuário de banco de dados.
GET PATCH DELETE	/security/users/{name}	O método GET permite recuperar todos os detalhes de um usuário, como nome, endereço de e-mail, função, tipo de autorização. O método DE PATCH permite atualizar os detalhes. O método DE ELIMINAÇÃO permite-lhe remover o utilizador.

## Visualização de métricas de desempenho usando APIs

O Active IQ Unified Manager fornece um conjunto de APIs `/datacenter` na categoria que permitem visualizar os dados de performance dos clusters e objetos de storage em um data center. Essas APIs recuperam os dados de performance de diferentes objetos de storage, como clusters, nós, LUNs, volumes, agregados, VMs de storage, interfaces FC, portas FC, portas Ethernet e interfaces IP.

``/metrics`` As APIs e ``/analytics`` oferecem visualizações diferentes das métricas de performance, usando as quais, você pode detalhar diferentes níveis de detalhes para os seguintes objetos de storage em seu data center:

- clusters
- nós
- VMs de storage
- agregados
- volumes
- LUNs
- Interfaces FC
- Portas FC

- Portas Ethernet
- Interfaces IP

A tabela a seguir desenha uma comparação entre o `/metrics` e as APIs com `/analytics` relação aos detalhes dos dados de desempenho recuperados.

<b>Métricas</b>	<b>Análises</b>
Detalhes de desempenho para um único objeto. Por exemplo, a <code>/datacenter/cluster/clusters/{key}/metrics</code> API exige que a chave de cluster seja inserida como parâmetro de caminho para recuperar as métricas desse cluster específico.	Detalhes de desempenho para vários objetos do mesmo tipo em um data center. Por exemplo, a <code>/datacenter/cluster/clusters/analytics</code> API recupera as métricas coletivas de todos os clusters em um data center.
Amostra de métricas de desempenho para um objeto de armazenamento com base no parâmetro de intervalo de tempo para recuperação.	O valor agregado de alto nível de performance para um determinado tipo de objeto de storage por um determinado período (acima de 72 horas).
Os detalhes básicos do objeto são recuperados, como detalhes de um nó ou cluster.	Nenhum detalhe específico é recuperado.
Contadores acumulados, como mínimo, máximo, percentil 95th e os valores médios de desempenho ao longo de um período de tempo, são recuperados para um único objeto, como contadores de leitura, escrita, total e outros.	Um único valor agregado é exibido para todos os objetos do mesmo tipo.

Métricas	Análises
<p>O intervalo de tempo e os dados de amostra baseiam-se no seguinte programa: O intervalo de tempo para os dados. Exemplos podem ser 1h, 12h, 1D, 2D, 3D, 15d, 1W, 1m, 2m, 3m, 6m. Você obtém amostras de 1 horas se o intervalo for mais de 3 dias (72 h) caso contrário são amostras de 5 minutos. O período para cada intervalo de tempo é o seguinte:</p> <ul style="list-style-type: none"> <li>• 1H: Métricas na hora mais recente amostrada ao longo de 5 minutos.</li> <li>• 12h: Métricas nas últimas 12 horas amostradas ao longo de 5 minutos.</li> <li>• 1D: Métricas no dia mais recente amostradas ao longo de 5 minutos.</li> <li>• 2D: Métricas nos últimos 2 dias amostradas ao longo de 5 minutos.</li> <li>• 3D: Métricas nos últimos 3 dias amostradas ao longo de 5 minutos.</li> <li>• 15D: Métricas nos últimos 15 dias amostrados ao longo de 1 hora.</li> <li>• 1W: As métricas na semana mais recente amostraram mais de 1 hora.</li> <li>• 1m: As métricas do mês mais recente amostraram mais de 1 hora.</li> <li>• 2M: Métricas nos últimos 2 meses amostradas ao longo de 1 hora.</li> <li>• 3M: Métricas nos últimos 3 meses amostradas ao longo de 1 hora.</li> <li>• 6m: Métricas nos últimos 6 meses amostradas ao longo de 1 hora.</li> </ul> <p>Valores disponíveis : 1h, 12h, 1D, 2D, 3D, 15d, 1W, 6m, 2m, 3m, 1m</p> <p>Valor padrão : 1h</p>	<p>Acima de 72 horas. A duração sobre a qual esta amostra é calculada é representada no formato padrão ISO-8601.</p>

### Amostra de saída para APIs de métricas

Por exemplo, a `/datacenter/cluster/nodes/{key}/metrics` API recupera os seguintes detalhes (entre outros) para um nó:



O percentil 95 no valor sumário indica que 95% das amostras coletadas para o período têm um valor de contador menor que o valor especificado como percentil 95.

```
{
```

```

    "iops": {
      "local": {
        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
      },
      "other": 100.53,
      "read": 100.53,
      "total": 100.53,
      "write": 100.53
    },
    "latency": {
      "other": 100.53,
      "read": 100.53,
      "total": 100.53,
      "write": 100.53
    },
    "performance_capacity": {
      "available_iops_percent": 0,
      "free_percent": 0,
      "system_workload_percent": 0,
      "used_percent": 0,
      "user_workload_percent": 0
    },
    "throughput": {
      "other": 100.53,
      "read": 100.53,
      "total": 100.53,
      "write": 100.53
    },
    "timestamp": "2018-01-01T12:00:00-04:00",
    "utilization_percent": 0
  }
],
"start_time": "2018-01-01T12:00:00-04:00",
"summary": {
  "iops": {
    "local_iops": {
      "other": {
        "95th_percentile": 28,
        "avg": 28,
        "max": 28,
        "min": 5
      },
      "read": {

```



```
    "95th_percentile": 28,  
    "avg": 28,  
    "max": 28,  
    "min": 5  
  },  
  "total": {  
    "95th_percentile": 28,  
    "avg": 28,  
    "max": 28,  
    "min": 5  
  },  
  "write": {  
    "95th_percentile": 28,  
    "avg": 28,  
    "max": 28,  
    "min": 5  
  }  
},
```

### Amostra de saída para APIs de análise

Por exemplo, a `/datacenter/cluster/nodes/analytics` API recupera os seguintes valores (entre outros) para todos os nós:

```

{
  "iops": 1.7471,
  "latency": 60.0933,
  "throughput": 5548.4678,
  "utilization_percent": 4.8569,
  "period": 72,
  "performance_capacity": {
    "used_percent": 5.475,
    "available_iops_percent": 168350
  },
  "node": {
    "key": "37387241-8b57-11e9-8974-00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a",
    "uuid": "95f94e8d-8b4e-11e9-8974-00a098e0219a",
    "name": "ocum-infinity-01",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/nodes/37387241-8b57-11e9-8974-00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a"
      }
    }
  },
  "cluster": {
    "key": "37387241-8b57-11e9-8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a",
    "uuid": "37387241-8b57-11e9-8974-00a098e0219a",
    "name": "ocum-infinity",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/37387241-8b57-11e9-8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a"
      }
    }
  },
  "_links": {
    "self": {
      "href": "/api/datacenter/cluster/nodes/analytics"
    }
  }
},
},

```

## Lista das APIs disponíveis

A tabela a seguir descreve `/metrics` as APIs e `/analytics` em detalhes.



As métricas de IOPS e performance retornadas por essas APIs são valores duplos, por 100.53 exemplo. A filtragem desses valores flutuantes pelos caracteres pipe (|) e curinga (\*) não é suportada.

<b>Verbo HTTP</b>	<b>Caminho</b>	<b>Descrição</b>
GET	/datacenter/cluster/clusters/{key}/metrics	Recupera dados de desempenho (amostra e resumo) para um cluster especificado pelo parâmetro de entrada da chave do cluster. Informações, como a chave do cluster e UUID, intervalo de tempo, IOPS, taxa de transferência e o número de amostras são retornadas.
GET	/datacenter/cluster/clusters/analytics	Recupera métricas de desempenho de alto nível para todos os clusters em um data center. Você pode filtrar seus resultados com base nos critérios necessários. Valores, como IOPS agregado, taxa de transferência e o período de coleta (em horas) são retornados.
GET	/datacenter/cluster/nodes/{key}/metrics	Recupera dados de desempenho (amostra e resumo) para um nó especificado pelo parâmetro de entrada da chave do nó. Informações, como UUID do nó, intervalo de tempo, resumo do IOPS, taxa de transferência, latência e desempenho, o número de amostras coletadas e a porcentagem utilizada são retornadas.
GET	/datacenter/cluster/nodes/analytics	Recupera métricas de desempenho de alto nível para todos os nós em um data center. Você pode filtrar seus resultados com base nos critérios necessários. Informações, como chaves de nó e cluster, e valores, como IOPS agregado, taxa de transferência e o período de coleta (em horas) são retornados.

<b>Verbo HTTP</b>	<b>Caminho</b>	<b>Descrição</b>
GET	/datacenter/storage/aggregates/{key}/metrics	Recupera dados de desempenho (amostra e resumo) para um agregado especificado pelo parâmetro de entrada da chave agregada. Informações, como o intervalo de tempo, o resumo do IOPS, a latência, a taxa de transferência e a capacidade de desempenho, o número de amostras coletadas para cada contador e a porcentagem utilizada são retornadas.
GET	/datacenter/storage/aggregates/analytics	Recupera métricas de desempenho de alto nível para todos os agregados em um data center. Você pode filtrar seus resultados com base nos critérios necessários. Informações, como chaves de agregado e cluster, e valores, como IOPS agregado, taxa de transferência e o período de coleta (em horas) são retornados.
GET	/datacenter/storage/luns/{key}/metrics  /datacenter/storage/volumes/{key}/metrics	Recupera dados de desempenho (amostra e resumo) para um LUN ou um compartilhamento de arquivo (volume) especificado pelo parâmetro de entrada da chave LUN ou volume. Informações, como o resumo do mínimo, máximo e média das IOPS de leitura, gravação e total, latência e taxa de transferência, e o número de amostras coletadas para cada contador são retornadas.
GET	/datacenter/storage/luns/analytics  /datacenter/storage/volumes/analytics	Recupera métricas de desempenho de alto nível para todos os LUNs ou volumes em um data center. Você pode filtrar seus resultados com base nos critérios necessários. Informações, como chaves de cluster e VM de storage, e valores, como IOPS agregado, taxa de transferência e o período de coleta (em horas) são retornados.

<b>Verbo HTTP</b>	<b>Caminho</b>	<b>Descrição</b>
GET	/datacenter/svm/svms/{key}/metrics	Recupera dados de desempenho (amostra e resumo) para uma VM de armazenamento especificada pelo parâmetro de entrada da chave VM de armazenamento. O resumo das IOPS com base em cada protocolo suportado, como <i>nvmf</i> , <i>fcp</i> , <i>iscsi</i> , <i>enfs</i> , taxa de transferência, latência e o número de amostras coletadas são retornados.
GET	/datacenter/svm/svms/analyt	Recupera métricas de desempenho de alto nível para todas as VMs de armazenamento em um data center. Você pode filtrar seus resultados com base nos critérios necessários. Informações, como UUID de VM de storage, IOPS agregado, latência, taxa de transferência e o período de coleta (em horas) são retornadas.
GET	/datacenter/network/ethernet/ports/{key}/metrics	Recupera as métricas de desempenho de uma porta ethernet específica especificada pelo parâmetro de entrada da chave de porta. Quando um intervalo (intervalo de tempo) é fornecido a partir do intervalo suportado, a API retorna os contadores acumulados, como valores mínimos, máximos e médios de desempenho durante o período de tempo.

Verbo HTTP	Caminho	Descrição
GET	/datacenter/network/ethernet/ports/analytics	Recupera as métricas de desempenho de alto nível para todas as portas ethernet em seu ambiente de data center. Informações, como a chave de cluster e nó e UUID, taxa de transferência, período de coleta e porcentagem de utilização das portas são retornadas. Você pode filtrar o resultado pelos parâmetros disponíveis, como chave de porta, porcentagem de utilização, nome de cluster e nó e UUID, e assim por diante.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Recupera as métricas de desempenho de uma interface FC de rede específica especificada pelo parâmetro de entrada da chave de interface. Quando um intervalo (intervalo de tempo) é fornecido a partir do intervalo suportado, a API retorna os contadores acumulados, como valores mínimos, máximos e médios de desempenho durante o período de tempo.
GET	/datacenter/network/fc/interfaces/analytics	Recupera as métricas de desempenho de alto nível para todas as portas ethernet em seu ambiente de data center. Informações, como a chave de interface FC e cluster e UUID, taxa de transferência, IOPS, latência e VM de storage, são retornadas. Você pode filtrar o resultado pelos parâmetros disponíveis, como o cluster e o nome da interface FC e UUID, VM de storage, taxa de transferência, etc.

<b>Verbo HTTP</b>	<b>Caminho</b>	<b>Descrição</b>
GET	/datacenter/network/fc/ports/{key}/metrics	Recupera as métricas de desempenho de uma porta FC específica especificada pelo parâmetro de entrada da chave de porta. Quando um intervalo (intervalo de tempo) é fornecido a partir do intervalo suportado, a API retorna os contadores acumulados, como valores mínimos, máximos e médios de desempenho durante o período de tempo.
GET	/datacenter/network/fc/ports/analytics	Recupera as métricas de desempenho de alto nível para todas as portas FC em seu ambiente de data center. Informações, como a chave de cluster e nó e UUID, taxa de transferência, período de coleta e porcentagem de utilização das portas são retornadas. Você pode filtrar o resultado pelos parâmetros disponíveis, como chave de porta, porcentagem de utilização, nome de cluster e nó e UUID, e assim por diante.
GET	/datacenter/network/ip/interfaces/{key}/metrics	Recupera as métricas de desempenho de uma interface IP de rede, conforme especificado pelo parâmetro de entrada da chave de interface. Quando um intervalo (intervalo de tempo) é fornecido a partir do intervalo suportado, a API retorna informações, como o número de amostras, contadores acumulados, taxa de transferência e o número de pacotes recebidos e transmitidos.

Verbo HTTP	Caminho	Descrição
GET	/datacenter/network/ip/interfaces/analytics	Recupera as métricas de desempenho de alto nível para todas as interfaces IP de rede em seu ambiente de data center. Informações, como a chave de interface IP e cluster e UUID, taxa de transferência, IOPS e latência são retornadas. Você pode filtrar o resultado pelos parâmetros disponíveis, como o cluster e o nome da interface IP e UUID, IOPS, latência, taxa de transferência e assim por diante.

## Visualização de trabalhos e detalhes do sistema

Você pode usar a `jobs API management-server` na categoria para exibir os detalhes de execução das operações assíncronas. A `system API management-server` na categoria permite exibir os detalhes da instância no ambiente do Active IQ Unified Manager.

### Exibindo trabalhos

No Active IQ Unified Manager, operações como adicionar e modificar recursos são executadas por invocações de API síncronas e assíncronas. As invocações agendadas para execução assíncrona podem ser rastreadas por um objeto Job criado para essa invocação. Cada objeto trabalho tem uma chave exclusiva para identificação. Cada objeto Job retorna o URI de objeto Job para você acessar e acompanhar o andamento do trabalho. Você pode usar essa API para recuperar os detalhes de cada execução.

Usando esta API, você pode consultar todos os objetos de trabalho para o seu data center, incluindo dados históricos. A consulta de todos os trabalhos, por padrão, retorna os detalhes dos últimos 20 trabalhos acionados através da interface web e API. Utilize os filtros incorporados para ver trabalhos específicos. Você também pode usar a tecla trabalho para consultar os detalhes de uma tarefa específica e executar o próximo conjunto de operações nos recursos.

Categoria	Verbo HTTP	Caminho	Descrição
servidor de gerenciamento	OBTER	/management-server/jobs	Retorna os detalhes do trabalho de todos os trabalhos. Sem qualquer ordem de classificação, o último objeto trabalho enviado é devolvido no topo.



<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>	<b>Descrição</b>
servidor de gerenciamento	OBTER	/management-server/jobs/{key}  Introduza a chave do trabalho do objeto trabalho para visualizar os detalhes específicos desse trabalho.	Retorna os detalhes do objeto Job específico.

### Visualização dos detalhes do sistema

Usando a `/management-server/system` API, você pode consultar os detalhes específicos da instância do seu ambiente do Unified Manager. A API retorna informações sobre o produto e os serviços, como a versão do Unified Manager instalada no sistema, UUID, nome do fornecedor, sistema operacional do host e o nome, descrição e status dos serviços executados na instância do Unified Manager.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>	<b>Descrição</b>
servidor de gerenciamento	OBTER	/management-server/system	Nenhum parâmetro de entrada é necessário para executar esta API. Os detalhes do sistema da instância atual do Unified Manager são retornados por padrão.

### Gerenciamento de eventos e alertas usando APIs

As `events`, `alerts` APIs e , na `management-server` categoria , `scripts` permitem gerenciar eventos, alertas e `scripts` associados aos alertas no ambiente do Active IQ Unified Manager.

#### Visualizar e modificar eventos

O Unified Manager recebe os eventos gerados no ONTAP para os clusters monitorados e gerenciados pelo Unified Manager. Usando essas APIs, você pode visualizar os eventos gerados para os clusters e resolvê-los e atualizá-los.

Ao executar o `GET` método para `/management-server/events` a API, você pode consultar os eventos em seu data center, incluindo dados históricos. Use os filtros incorporados, como nome, nível de impactos, área de impactos, gravidade, estado, nome do recurso e tipo de recurso, para visualizar eventos específicos. Os parâmetros de tipo e área de recurso retornam informações sobre o objeto de armazenamento no qual o evento ocorreu, e a área de impactos retorna as informações sobre o problema para o qual o evento é gerado, como disponibilidade, capacidade, configuração, segurança, proteção e desempenho.

Ao executar a OPERAÇÃO DE PATCH para esta API, você pode ativar o fluxo de trabalho de resolução para o evento. Você pode atribuir um evento a si mesmo ou a outro usuário e confirmar o recebimento do evento. Ao executar as etapas nos recursos para resolver o problema que acionou o evento, você pode usar essa API para marcar o evento como resolvido.

Para obter mais informações sobre eventos, "[Gerenciamento de eventos](#)" consulte .

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>	<b>Descrição</b>
servidor de gerenciamento	GET	<code>/management-server/events</code> <code>/management-server/events/{key}</code>	Quando você executa o método Get ALL, o corpo de resposta consiste nos detalhes do evento de todos os eventos em seu data center. Ao recuperar os detalhes do evento por uma chave específica, você pode exibir os detalhes de um evento específico e executar o próximo conjunto de operações nos recursos. O corpo de resposta consiste nos detalhes desse evento.
servidor de gerenciamento	PATCH	<code>management-server/events/{key}</code>	Execute esta API para atribuir um evento ou alterar o estado para reconhecido ou resolvido. Você também pode usar esse método para atribuir o evento a você mesmo ou a outro usuário. É uma operação síncrona.

## Gerenciamento de alertas

Os eventos são gerados automaticamente e continuamente. O Unified Manager gera um alerta somente quando um evento atende a determinados critérios de filtro. Você pode selecionar os eventos para os quais os alertas devem ser gerados. Usando a `/management-server/alerts` API, você pode configurar alertas para enviar notificações automaticamente quando eventos ou eventos específicos de determinados tipos de gravidade ocorrerem.

Para obter mais informações sobre alertas, "[Gerenciamento de alertas](#)" consulte .

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>	<b>Descrição</b>
servidor de gerenciamento	OBTER	/management-server/alerts /management-server/alerts/{key}	Consulte todos os alertas existentes em seu ambiente ou um alerta específico, usando a chave de alerta. Você pode exibir as informações sobre os alertas gerados em seu ambiente, como a descrição do alerta, ação, ID de e-mail para o qual a notificação é enviada, evento e gravidade.
servidor de gerenciamento	POST	/management-server/alerts	Este método permite adicionar alertas para eventos específicos. Você deve adicionar o nome do alerta, o recurso físico ou lógico ou evento no qual o alerta é aplicável, se o alerta está ativado e se você está emitindo traps SNMP. Você pode adicionar detalhes adicionais para os quais deseja gerar o alerta, como a ação, ID de e-mail de notificação, os detalhes do script, caso você esteja adicionando um script de alerta, e assim por diante.
servidor de gerenciamento	CORRIGIR e EXCLUIR	management-server/events/{key}	Você pode usar esses métodos para modificar e excluir alertas específicos. Você pode modificar atributos diferentes, como descrição, nome e ativar e desativar o alerta. Pode eliminar um alerta quando o alerta já não for necessário.



Ao selecionar um recurso para adicionar um alerta, observe que a seleção de um cluster como recurso não seleciona automaticamente os objetos de armazenamento dentro desse cluster. Por exemplo, se você criar um alerta para todos os eventos críticos para todos os clusters, receberá alertas apenas para eventos críticos do cluster. Você não receberá alertas de eventos críticos em nós, agregados e assim por diante.

## Gerenciamento de scripts

Usando a `/management-server/scripts` API, você também pode associar um alerta a um script que é executado quando um alerta é acionado. Você pode usar scripts para modificar ou atualizar automaticamente vários objetos de armazenamento no Unified Manager. O script está associado a um alerta. Quando um evento aciona um alerta, o script é executado. Você pode carregar scripts personalizados e testar sua execução quando um alerta é gerado. Você pode associar um alerta ao script para que o script seja executado quando um alerta for gerado para um evento no Unified Manager.

Para obter mais informações sobre scripts, "[Gerenciamento de scripts](#)" consulte .

Categoria	Verbo HTTP	Caminho	Descrição
servidor de gerenciamento	GET	<code>/management-server/scripts</code>	Use esta API para consultar todos os scripts existentes em seu ambiente. Use o filtro padrão e ordem por operações para exibir apenas scripts específicos.
servidor de gerenciamento	POST	<code>/management-server/scripts</code>	Use esta API para adicionar uma descrição para o script e fazer o upload do arquivo de script associado a um alerta.

## Gerenciamento de workloads usando APIs

As APIs descritas aqui abrangem várias funções de administração de storage, como visualização de workloads de storage, criação de LUNs e compartilhamentos de arquivos, gerenciamento de níveis de Serviço de Performance e políticas de eficiência de storage e atribuição de políticas para workloads de storage.

### Visualização de workloads de storage usando APIs

As APIs listadas aqui permitem visualizar uma lista consolidada de workloads de storage para todos os clusters do ONTAP no data center. As APIs também fornecem uma visualização resumida do número de workloads de storage provisionados no ambiente Active IQ Unified Manager e das estatísticas de capacidade e performance (IOPS).

## Visualizar workloads de storage

Use o método a seguir para visualizar todos os workloads de storage em todos os clusters do data center. Para obter informações sobre como filtrar a resposta com base em colunas específicas, consulte a documentação de referência da API disponível na instância do Unified Manager.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de storage	GET	/storage-provider/workloads

## Veja o resumo dos workloads de storage

Use o método a seguir para avaliar a capacidade usada, a capacidade disponível, o IOPS usado, o IOPS disponível e o número de workloads de storage gerenciados por cada nível de Serviço de Performance. Os workloads de storage exibidos podem ser para qualquer LUN, compartilhamento de arquivos NFS ou compartilhamento CIFS. A API fornece uma visão geral dos workloads de storage, uma visão geral dos workloads de storage provisionados pelo Unified Manager, uma visão geral do data center, uma visão geral do espaço total, usado e disponível e IOPS no data center, em termos de níveis de serviço de performance atribuídos. As informações recebidas em resposta a essa API são usadas para preencher o painel na IU do Unified Manager.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de storage	GET	/storage-provider/workloads-summary

## Gerenciamento de endpoints de acesso usando APIs

Você precisa criar pontos de extremidade de acesso ou interfaces lógicas (LIFs), que são necessárias para provisionar máquinas virtuais de storage (SVMs), LUNs e compartilhamentos de arquivos. Você pode exibir, criar, modificar e excluir os pontos de extremidade de acesso para SVMs, LUNs ou compartilhamentos de arquivos em seu ambiente Active IQ Unified Manager.

### Exibir endpoints de acesso

Você pode exibir uma lista dos pontos de extremidade de acesso no ambiente do Unified Manager usando o método a seguir. Para consultar uma lista de pontos de extremidade de acesso de um determinado SVM, LUN ou compartilhamento de arquivos, você precisa inserir o identificador exclusivo para o SVM, LUN ou compartilhamento de arquivos. Você também pode inserir a chave de endpoint de acesso exclusiva para recuperar os detalhes do endpoint de acesso específico.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de storage	GET	/storage-provider/access-endpoints  /storage-provider/access-endpoints/{key}

### Adicione pontos de extremidade de acesso

Você pode criar endpoints de acesso personalizados e atribuir propriedades necessárias a ele. Você deve inserir os detalhes do endpoint de acesso que deseja criar como parâmetros de entrada. Você pode usar essa API, o Gerenciador de sistema ou a CLI do ONTAP para criar um ponto de extremidade de acesso em cada nó. Os endereços IPv4 e IPv6 são suportados para a criação de endpoints de acesso.



É necessário configurar o SVM com um número mínimo de pontos de extremidade de acesso por nó para o provisionamento bem-sucedido de LUNs e compartilhamentos de arquivos. Você deve configurar o SVM com pelo menos dois pontos de extremidade de acesso por nó, um com suporte ao protocolo CIFS e/ou NFS, outro com suporte ao protocolo iSCSI ou FCP.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de storage	POST	/storage-provider/access-endpoints

### Eliminar pontos de extremidade de acesso

Você pode excluir um endpoint de acesso específico usando o seguinte método. Você precisa fornecer a chave de endpoint de acesso como um parâmetro de entrada para excluir um endpoint de acesso específico.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de storage	ELIMINAR	/storage-provider/access-endpoints/{key}

### Modificar endpoints de acesso

Você pode modificar um endpoint de acesso e atualizar suas propriedades usando o seguinte método. Você precisa fornecer a chave de endpoint de acesso para modificar um endpoint de acesso específico. Você também precisa inserir a propriedade que deseja atualizar, juntamente com seu valor.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de storage	PATCH	/storage-provider/access-endpoints/{key}

### Gerenciamento do mapeamento do ativo Directory usando APIs

Você pode usar as APIs listadas aqui para gerenciar mapeamentos do ativo Directory no SVM que são necessários para provisionar compartilhamentos CIFS nas SVMs. Os mapeamentos do ativo Directory precisam ser configurados para mapear os SVMs com o ONTAP.

### Exibir mapeamentos do ativo Directory

Você pode exibir os detalhes de configuração dos mapeamentos do ativo Directory para um SVM usando o método a seguir. Para visualizar os mapeamentos do ativo Directory em um SVM, é necessário inserir a chave SVM. Para consultar os detalhes de um mapeamento específico, você deve inserir a chave de mapeamento.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de armazenamento	OBTER	/storage-provider/active-directories-mappings  /storage-provider/active-directories-mappings/{key}

#### Adicionar mapeamento do ativo Directory

Você pode criar mapeamentos do ativo Directory em um SVM usando o método a seguir. Você deve inserir os detalhes do mapeamento como os parâmetros de entrada.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de armazenamento	POST	/storage-provider/active-directories-mappings

#### Gerenciamento de compartilhamentos de arquivos usando APIs

Você pode usar a `/storage-provider/file-shares` API para exibir, adicionar, modificar e excluir os volumes de compartilhamento de arquivos CIFS e NFS em seu ambiente de data center.

Antes de provisionar os volumes de compartilhamento de arquivos, verifique se o SVM foi criado e provisionado com os protocolos compatíveis. Se você estiver atribuindo níveis de Serviço de desempenho (PSLs) ou políticas de eficiência de armazenamento (SEPs), durante o provisionamento, as PSLs ou SEPs devem ser criadas antes de criar os compartilhamentos de arquivo.

#### Ver compartilhamentos de arquivo

Você pode usar o método a seguir para exibir os volumes de compartilhamento de arquivos disponíveis no ambiente do Unified Manager. Quando você adicionou um cluster do ONTAP como fonte de dados no Active IQ Unified Manager, as cargas de trabalho de armazenamento desses clusters são adicionadas automaticamente à instância do Unified Manager. Essa API recupera os compartilhamentos de arquivo automaticamente e manualmente adicionados à instância do Unified Manager. Você pode exibir os detalhes de um compartilhamento de arquivos específico executando essa API com a chave de compartilhamento de arquivos.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de armazenamento	OBTER	/storage-provider/file-shares  /storage-provider/file-shares/{key}

#### Adicionar compartilhamentos de arquivo

Use o método a seguir para adicionar compartilhamentos de arquivos CIFS e NFS no SVM. Você deve inserir

os detalhes do compartilhamento de arquivo que deseja criar, como os parâmetros de entrada. Você não pode usar essa API para adicionar volumes do FlexGroup.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	POST	/storage-provider/file-shares



Dependendo se os parâmetros da lista de controle de acesso (ACL) ou os parâmetros da política de exportação são fornecidos, compartilhamentos CIFS ou compartilhamentos de arquivos NFS são criados. Se você não fornecer os valores para os parâmetros ACL, compartilhamentos CIFS não serão criados e compartilhamentos NFS serão criados por padrão, fornecendo acesso a todos.

**Criando volumes de proteção de dados:** Quando você adiciona compartilhamentos de arquivo ao SVM, o tipo de volume montado, por padrão, é `rw` (leitura-gravação). Para criar volumes de proteção de dados (DP), especifique `dp` como o valor para o `type` parâmetro.

#### Excluir compartilhamentos de arquivo

Você pode usar o seguinte método para excluir um compartilhamento de arquivo específico. Você precisa inserir a chave de compartilhamento de arquivo como um parâmetro de entrada para excluir um compartilhamento de arquivo específico.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	ELIMINAR	/storage-provider/file-shares/{key}

#### Modificar compartilhamentos de arquivo

Você pode usar o seguinte método para modificar um compartilhamento de arquivo e atualizar suas propriedades.

Você precisa fornecer a chave de compartilhamento de arquivo para modificar um compartilhamento de arquivo específico. Além disso, você precisa inserir a propriedade que deseja atualizar, juntamente com seu valor.



Observe que você pode atualizar apenas uma propriedade em uma única invocação desta API. Para várias atualizações, você precisa executar essa API quantas vezes.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	PATCH	/storage-provider/file-shares/{key}

#### Gerenciamento de LUNs usando APIs

Você pode usar a `/storage-provider/luns` API para exibir, adicionar, modificar e excluir os LUNs no ambiente de data center.



Antes de provisionar os LUNs, verifique se o SVM foi criado e provisionado com os protocolos compatíveis. Se você estiver atribuindo níveis de Serviço de desempenho (PSLs) ou políticas de eficiência de armazenamento (SEPs), durante o provisionamento, as PSLs ou SEPs devem ser criadas antes de criar o LUN.

### Ver LUNs

Use o método a seguir para exibir os LUNs no ambiente do Unified Manager. Quando você adicionou um cluster do ONTAP como fonte de dados no Active IQ Unified Manager, as cargas de trabalho de storage desses clusters são adicionadas automaticamente à instância do Unified Manager. Essa API recupera todos os LUNs adicionados automaticamente e manualmente à instância do Unified Manager. Você pode exibir os detalhes de um LUN específico executando esta API com a chave LUN.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	OBTER	/storage-provider/luns  /storage-provider/luns/{key}

### Adicionar LUNs

Você pode usar o método a seguir para adicionar LUNs às SVMs.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	POST	/storage-provider/luns



Em sua solicitação curl, se você fornecer um valor para o parâmetro opcional `volume_name_tag` na entrada, esse valor será usado ao nomear o volume durante a criação de LUN. Esta etiqueta permite pesquisar o volume facilmente. Se você fornecer a chave de volume na solicitação, a marcação será ignorada.

### Eliminar LUNs

Você pode usar o seguinte método para excluir um LUN específico. Você precisa fornecer a chave LUN para excluir um LUN específico.



Se você tiver criado um volume no ONTAP e provisionado LUNs por meio do Gerenciador Unificado nesse volume, ao excluir todos os LUNs usando essa API, o volume também será excluído do cluster do ONTAP.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	ELIMINAR	/storage-provider/luns/{key}

### Modificar LUNs

Você pode usar o seguinte método para modificar um LUN e atualizar suas propriedades. Você precisa fornecer a chave LUN para modificar um LUN específico. Você também precisa inserir a propriedade LUN que

deseja atualizar, juntamente com seu valor. Para atualizar arrays LUN usando essa API, você deve revisar as recomendações em "recomendações para usar as APIs".



Você pode atualizar apenas uma propriedade em uma única invocação desta API. Para várias atualizações, você precisa executar essa API quantas vezes.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	PATCH	/storage-provider/luns/{key}

### Gerenciamento de níveis de serviço de performance usando APIs

Você pode exibir, criar, modificar e excluir níveis de Serviço de desempenho usando as APIs do provedor de armazenamento no Active IQ Unified Manager.

#### Ver níveis de Serviço de desempenho

Você pode usar o método a seguir para exibir os níveis de Serviço de Performance para atribuí-los a cargas de trabalho de storage. A API lista todos os níveis de Serviço de desempenho definidos pelo sistema e criados pelo usuário e recupera os atributos de todos os níveis de Serviço de desempenho. Se pretender consultar um nível de Serviço de desempenho específico, tem de introduzir a ID exclusiva do nível de Serviço de desempenho para obter os respetivos detalhes.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	OBTER	/storage-provider/performance-service-levels  /storage-provider/performance-service-levels/{key}

#### Adicione níveis de serviço de desempenho

Use o método a seguir para criar níveis de serviço de performance personalizados e atribuí-los aos workloads de storage se os níveis de serviço de performance definidos pelo sistema não atenderem aos objetivos de nível de serviço (SLOs) necessários para os workloads de storage. Insira os detalhes do nível de Serviço de desempenho que você deseja criar. Para as propriedades IOPS, certifique-se de inserir um intervalo válido de valores.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	POST	/storage-provider/performance-service-levels

### Eliminar níveis de Serviço de desempenho

Você pode usar o seguinte método para excluir um nível de Serviço de desempenho específico. Não é possível excluir um nível de Serviço de desempenho se ele for atribuído a uma carga de trabalho ou se for o único nível de Serviço de desempenho disponível. Você precisa fornecer o ID exclusivo do nível de Serviço de desempenho como um parâmetro de entrada para excluir um nível de Serviço de desempenho específico.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de storage	ELIMINAR	/storage-provider/performance-service-levels/{key}

### Modificar níveis de Serviço de desempenho

Você pode usar o seguinte método para modificar um nível de Serviço de desempenho e atualizar suas propriedades. Não é possível modificar um nível de Serviço de Performance definido pelo sistema ou atribuído a uma carga de trabalho. Você precisa fornecer o ID exclusivo do para modificar um nível de Serviço de desempenho específico. Você também deve inserir a propriedade IOPS que deseja atualizar, juntamente com um valor válido.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de storage	PATCH	/storage-provider/performance-service-levels/{key}

### Visualização de recursos agregados com base nos níveis de Serviço de Performance

Você pode usar o método a seguir para consultar os recursos agregados com base nos níveis de Serviço de desempenho. Essa API retorna a lista de agregados disponíveis em seu data center e indica os recursos em termos de níveis de Serviço de desempenho que podem ser suportados nesses agregados. Ao provisionar workloads em um volume, você pode visualizar a funcionalidade de um agregado para dar suporte a um nível de Serviço de Performance específico e provisionar workloads com base nessa funcionalidade. Sua capacidade de especificar o agregado está disponível somente quando você está provisionando uma carga de trabalho usando APIs. Essa funcionalidade não está disponível na IU da Web do Unified Manager.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de storage	OBTER	/storage-provider/aggregate-capabilities  /storage-provider/aggregate-capabilities/{key}

### Gerenciamento de políticas de eficiência de storage usando APIs

Você pode exibir, criar, modificar e excluir políticas de eficiência de storage usando as APIs do provedor de storage.

Observe os seguintes pontos:



- Não é obrigatório atribuir uma Política de eficiência de storage ao criar um workload no Unified Manager.
- Não é possível anular a atribuição de uma Política de eficiência de armazenamento de uma carga de trabalho depois de uma política ser atribuída a ela.
- Se um workload tiver algumas configurações de storage especificadas em volumes do ONTAP, como deduplicação e compactação, essas configurações poderão ser sobrescritas pelas configurações especificadas na Política de eficiência de storage aplicada quando você adicionar os workloads de storage no Unified Manager.

#### Ver políticas de eficiência de storage

Você pode usar o método a seguir para visualizar as políticas de eficiência de storage antes de atribuí-las a workloads de storage. Esta API lista todas as políticas de eficiência de armazenamento definidas pelo sistema e criadas pelo usuário e recupera os atributos de todas as políticas de eficiência de armazenamento. Se você quiser consultar uma Política de eficiência de armazenamento específica, você precisa inserir o ID exclusivo da política para recuperar seus detalhes.

Categoria	Verbo HTTP	Caminho
provedor de storage	GET	<code>/storage-provider/storage-efficiency-policies</code>  <code>/storage-provider/storage-efficiency-policies/{key}</code>

#### Adicione políticas de eficiência de storage

Use o método a seguir para criar políticas de eficiência de storage personalizadas e atribuí-las aos workloads de storage se as políticas definidas pelo sistema não atenderem aos requisitos de provisionamento para seus workloads de storage. Insira os detalhes da Política de eficiência de armazenamento que você deseja criar, como parâmetros de entrada.

Categoria	Verbo HTTP	Caminho
provedor de storage	POST	<code>/storage-provider/storage-efficiency-policies</code>

#### Excluir políticas de eficiência de storage

Você pode usar o seguinte método para excluir uma Política de eficiência de armazenamento específica. Não é possível excluir uma Política de eficiência de storage se ela for atribuída a uma carga de trabalho ou se for a única Política de eficiência de storage disponível. Você precisa fornecer o ID exclusivo da Política de eficiência de armazenamento como um parâmetro de entrada para excluir uma Política de eficiência de armazenamento específica.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
fornecedor de storage	ELIMINAR	/storage-provider/storage-efficiency-policies/{key}

### Modificar políticas de eficiência de storage

Você pode usar o seguinte método para modificar uma Política de eficiência de armazenamento e atualizar suas propriedades. Não é possível modificar uma Política de eficiência de storage definida pelo sistema ou atribuída a uma carga de trabalho. Você precisa fornecer o ID exclusivo da Política de eficiência de storage para modificar uma Política de eficiência de storage específica. Além disso, você precisa fornecer a propriedade que você deseja atualizar, juntamente com seu valor.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
fornecedor de storage	PATCH	/storage-provider/storage-efficiency-policies/{key}

## Workflows de API comuns para gerenciamento de storage

Os fluxos de trabalho comuns fornecem aos desenvolvedores de aplicativos clientes exemplos de como as APIs do Active IQ Unified Manager podem ser chamadas por um aplicativo cliente para executar funções comuns de gerenciamento de storage. Esta seção contém alguns desses fluxos de trabalho de amostra.

Os fluxos de trabalho descrevem alguns dos casos de uso de gerenciamento de armazenamento comumente usados, juntamente com códigos de exemplo para você usar. Cada uma das tarefas é descrita usando um processo de fluxo de trabalho que consiste em uma ou mais chamadas de API.

### Entendendo as chamadas de API usadas nos fluxos de trabalho

Você pode exibir a página de documentação on-line da instância do Unified Manager que inclui os detalhes de cada chamada de API REST. Este documento não repete os detalhes da documentação online. Cada chamada de API usada nos exemplos de fluxo de trabalho neste documento inclui apenas as informações necessárias para localizar a chamada na página de documentação. Depois de localizar uma chamada de API específica, você pode revisar os detalhes completos da chamada, incluindo os parâmetros de entrada, formatos de saída, códigos de status HTTP e tipo de processamento de solicitação.

As seguintes informações são incluídas para cada chamada de API dentro de um fluxo de trabalho para ajudar a localizar a chamada na página de documentação:

- **Categoria:** As chamadas de API são organizadas na página de documentação em áreas ou categorias funcionalmente relacionadas. Para localizar uma chamada de API específica, role até a parte inferior da página e clique na categoria de API aplicável.
- **HTTP verb (chamada):** O verbo HTTP identifica a ação executada em um recurso. Cada chamada de API é executada através de um único verbo HTTP.
- **Caminho:** O caminho determina o recurso específico ao qual a ação se aplica como parte da execução de uma chamada. A cadeia de caracteres do caminho é anexada ao URL principal para formar a URL completa que identifica o recurso.

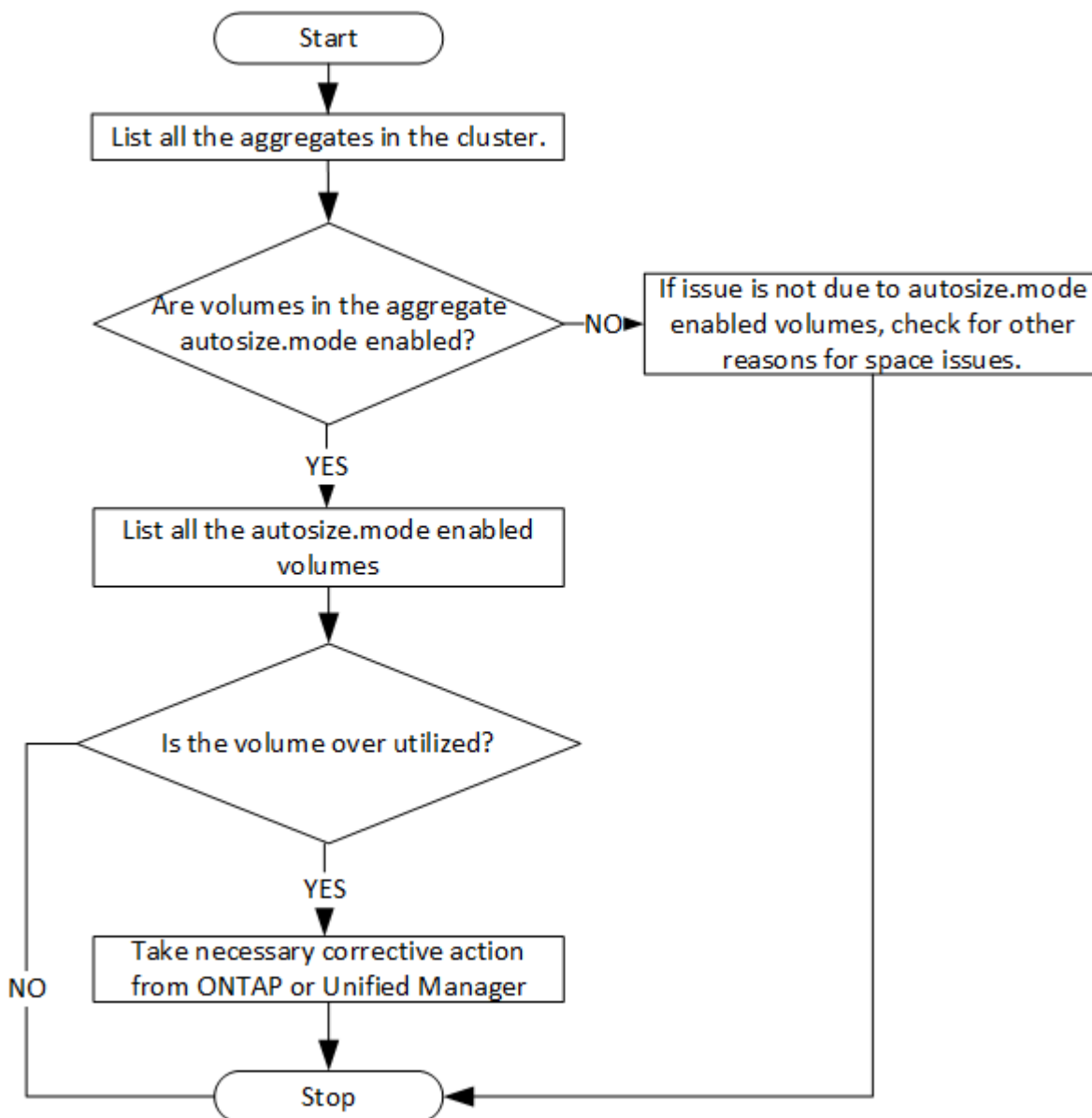
## Determinando problemas de espaço em agregados usando APIs

Use as APIs do data center no Active IQ Unified Manager para monitorar a disponibilidade e a utilização do espaço nos volumes. Você pode determinar problemas de espaço em seu volume e identificar recursos de storage que estão sobreutilizados ou subutilizados.

As APIs de data center para agregados recuperam as informações relevantes sobre o espaço disponível e usado e as configurações de eficiência de economia de espaço. Você também pode filtrar as informações recuperadas com base em atributos especificados.

Um método para determinar a falta de espaço em seus agregados é verificar se há volumes em seu ambiente com o modo automático ativado. Em seguida, você deve identificar quais volumes estão sendo sobreutilizados e executar quaisquer ações corretivas.

O fluxograma a seguir ilustra o processo de recuperação de informações sobre volumes com o modo automático ativado:



Esse fluxo pressupõe que os clusters já tenham sido criados no ONTAP e adicionados ao Unified Manager.

1. Obtenha a chave do cluster, a menos que você saiba o valor:

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
data center	OBTER	/datacenter/cluster/clusters

2. Usando a chave de cluster como parâmetro de filtro, consulte os agregados nesse cluster.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
data center	OBTER	/datacenter/storage/aggregates

3. A partir da resposta, analisar o uso do espaço dos agregados e determinar quais agregados têm problemas de espaço. Para cada agregado com problema de espaço, obtenha a chave agregada da mesma saída JSON.
4. Usando cada chave agregada, filtre todos os volumes que têm o valor para o parâmetro automático.mododo como grow.

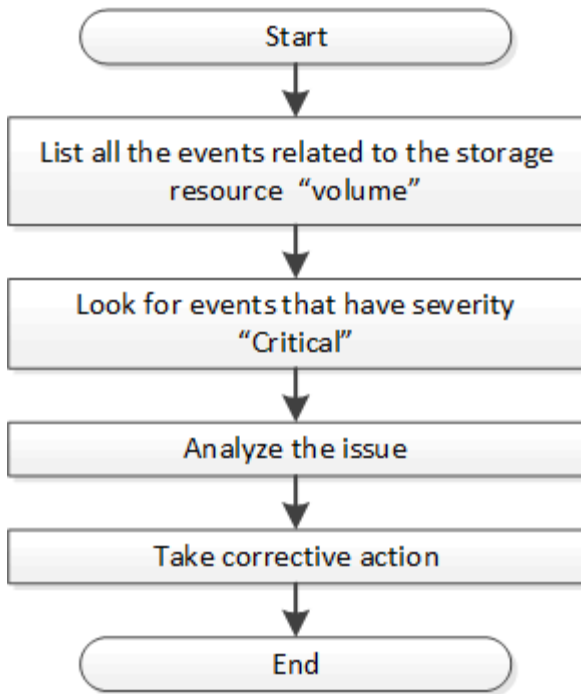
<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
data center	OBTER	/datacenter/storage/volumes

5. Analise quais volumes estão sendo sobreutilizados.
6. Execute qualquer ação corretiva necessária, como mover o volume entre agregados, para resolver os problemas de espaço em seu volume. Você pode executar essas ações na IU da Web do ONTAP ou do Unified Manager.

## Determinando problemas em objetos de storage usando APIs de eventos

Quando um objeto de storage no data center atravessa um limite, você recebe uma notificação sobre esse evento. Usando essa notificação, você pode analisar o problema e tomar medidas corretivas usando as `events` APIs.

Esse fluxo de trabalho toma o exemplo de um volume como objeto de recurso. Você pode usar as `events` APIs para recuperar a lista de eventos relacionados a um volume, analisar os problemas críticos para esse volume e, em seguida, tomar medidas corretivas para corrigir o problema.



Siga estas etapas para determinar os problemas em seu volume antes de tomar as medidas corretivas.

**Passos**

1. Analise as notificações de eventos críticos do Active IQ Unified Manager para os volumes em seu data center.
2. Consulte todos os eventos para os volumes usando os seguintes parâmetros na API /Management-server/events:

```

"resource_type": "volume"
"severity": "critical"
  
```

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
servidor de gerenciamento	OBTER	/management-server/events

3. Visualize a saída e analise os problemas nos volumes específicos.
4. Execute as ações necessárias usando as APIs REST do Unified Manager ou a IU da Web para resolver os problemas.

**Solução de problemas de volumes do ONTAP usando APIs de gateway**

As APIs de gateway atuam como um gateway para invocar as APIs do ONTAP para consultar informações sobre seus objetos de armazenamento do ONTAP e tomar medidas corretivas para solucionar os problemas relatados.

Esse fluxo de trabalho ocupa um exemplo de caso de uso no qual um evento é gerado quando um volume ONTAP quase atinge sua capacidade. O fluxo de trabalho também demonstra como resolver esse problema invocando uma combinação de APIs REST do Active IQ Unified Manager e do ONTAP.

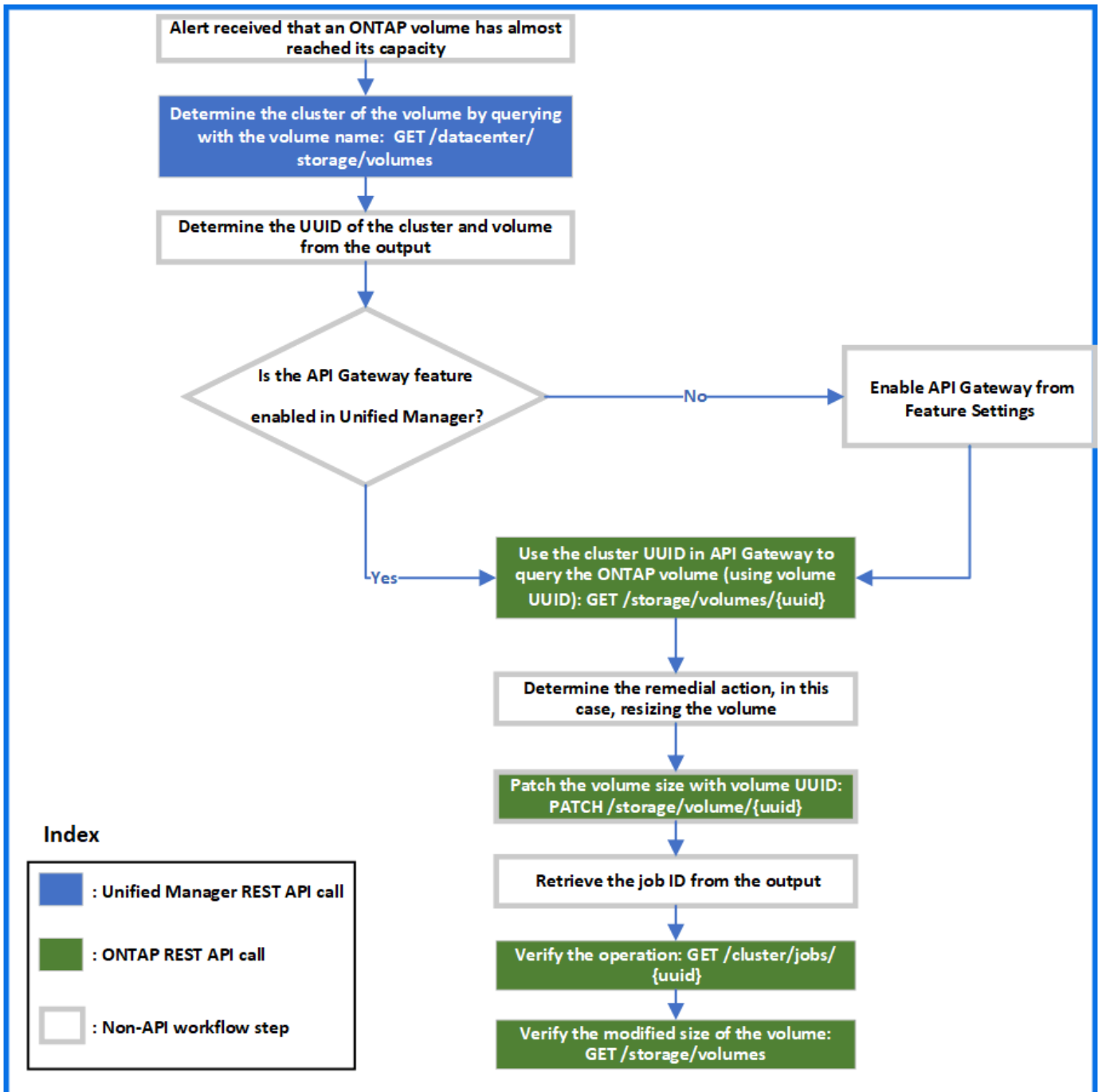


Antes de executar as etapas do fluxo de trabalho, verifique o seguinte:



- Você está ciente das APIs de gateway e como elas são usadas. Para obter informações, "[Acessando APIs do ONTAP por meio de acesso proxy](#)" consulte .
- Você está ciente do uso das APIs REST do ONTAP. Para obter informações sobre como usar APIS REST do ONTAP, "[Documentação de automação do ONTAP](#)" consulte .
- Você é um administrador de aplicativos.
- O cluster no qual você deseja executar as operações da API REST é compatível com o ONTAP 9.5 ou posterior, e o cluster é adicionado ao Unified Manager em HTTPS.

O diagrama a seguir ilustra cada etapa do fluxo de trabalho para solucionar o problema do uso da capacidade de volume do ONTAP.



O fluxo de trabalho abrange os pontos de invocação das APIs REST do Unified Manager e do ONTAP.

1. Anote o nome do volume do evento notificando a utilização da capacidade do volume.
2. Usando o nome do volume como o valor no parâmetro name, consulte o volume executando a seguinte API do Unified Manager.

Categoria	Verbo HTTP	Caminho
data center	OBTER	/datacenter/storage/volumes

3. Recupere o UUID do cluster e UUUID do volume da saída.
4. Na IU da Web do Unified Manager, navegue até **Geral > Configurações de recursos > Gateway de API** para verificar se o recurso API Gateway está ativado. A menos que esteja habilitado, as APIs sob a categoria gateway não estarão disponíveis para você invocar. Ative o recurso se ele estiver desativado.
5. Use o UUUID do cluster para executar a API ONTAP `/storage/volumes/{uuid}` por meio do gateway API. A consulta retorna os detalhes do volume quando o UUID do volume é passado como o parâmetro API.

Para executar as APIs do ONTAP por meio do gateway API, as credenciais do Unified Manager são passadas internamente para autenticação e você não precisa executar uma etapa adicional de autenticação para acesso individual ao cluster.

Categoria	Verbo HTTP	Caminho
Unified Manager: gateway ONTAP: Armazenamento	OBTER	API Gateway: /gateways/{uuid}/{path}  API do ONTAP: /storage/volumes/{uuid}



Em `/gateways/"uuuid"/"caminho"`, o valor para "uuid" deve ser substituído pelo cluster UUID no qual a operação RESTANTE deve ser executada. O caminho deve ser substituído pelo URL REST do ONTAP `/storage/volumes/`.

O URL anexado é: `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

Ao executar a operação GET, o URL gerado é:

`GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes/{volume_uuid}`

- Sample curl comando\*

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

6. A partir da saída, determine o tamanho, o uso e a medida corretiva a ser tomada. Neste fluxo de trabalho, a medida corretiva tomada é redimensionar o volume.

7. Use o UUID do cluster e execute a seguinte API do ONTAP através do gateway da API para redimensionar o volume. Para obter informações sobre os parâmetros de entrada para o gateway e as APIs do ONTAP, consulte a etapa 5.

Categoria	Verbo HTTP	Caminho
Unified Manager: gateway ONTAP: Armazenamento	PATCH	API Gateway: /gateways/{uuid}/{path}  API do ONTAP: /storage/volumes/{uuid}



Juntamente com o cluster UUID e UUID de volume, você deve inserir um valor para o parâmetro tamanho para redimensionar o volume. Certifique-se de inserir o valor *em bytes*. Por exemplo, se você quiser aumentar o tamanho de um volume de 100 GB para 120 GB, digite o valor do tamanho do parâmetro no final da consulta: `-d {"size": 128849018880}"`

- Sample curl comando\*

```
curl -X PATCH "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>" -d {"size": 128849018880}"
```

+

A saída JSON retorna um UUID de trabalho.

8. Verifique se a tarefa foi executada com êxito usando o UUID da tarefa. Use o UUID do cluster e UUID da tarefa para executar a seguinte API do ONTAP através do gateway da API. Para obter informações sobre os parâmetros de entrada para o gateway e as APIs do ONTAP, consulte a etapa 5.

Categoria	Verbo HTTP	Caminho
Unified Manager: gateway ONTAP: Cluster	GET	API Gateway: /gateways/{uuid}/{path}  API do ONTAP: /cluster/jobs/{uuid}

Os códigos HTTP retornados são os mesmos que os códigos de status HTTP API REST do ONTAP.

9. Execute a seguinte API ONTAP para consultar os detalhes do volume redimensionado. Para obter informações sobre os parâmetros de entrada para o gateway e as APIs do ONTAP, consulte a etapa 5.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
Unified Manager: gateway ONTAP: Armazenamento	OBTER	API Gateway: /gateways/{uuid}/{path}  API do ONTAP: /storage/volumes/{uuid}

A saída exibe um tamanho de volume aumentado de 120 GB.

## Workflows de API para gerenciamento de workload

Com o Active IQ Unified Manager, você pode provisionar e modificar workloads de storage (LUNs, compartilhamentos de arquivos NFS e compartilhamentos CIFS). O provisionamento consiste em várias etapas, desde a criação da Storage Virtual Machine (SVM) até a aplicação de políticas de nível de serviço de performance e eficiência de storage nos workloads de storage. A modificação de cargas de trabalho consiste nas etapas para modificar parâmetros específicos e habilitar recursos adicionais neles.

Os seguintes fluxos de trabalho são descritos:

- Fluxo de trabalho para provisionar máquinas virtuais de storage (SVMs) no Unified Manager.



Esse fluxo de trabalho deve ser executado antes de provisionar LUNs ou compartilhamentos de arquivos no Unified Manager.

- Provisionamento de compartilhamentos de arquivo.
- Provisionamento de LUNs.
- Modificação de LUNs e compartilhamentos de arquivos (usando o exemplo para atualizar o parâmetro Performance Service Level para os workloads de storage).
- Modificação de um compartilhamento de arquivos NFS para dar suporte ao protocolo CIFS
- Modificação de workloads para atualizar a QoS para AQoS



Para cada fluxo de trabalho de provisionamento (LUN e compartilhamentos de arquivos), certifique-se de que você tenha concluído o fluxo de trabalho para verificar os SVMs nos clusters.

Você também deve ler as recomendações e limitações antes de usar cada API nos fluxos de trabalho. Os detalhes relevantes das APIs estão disponíveis em suas seções individuais listadas nos conceitos e referências relacionados.

### Verificação de SVMs em clusters usando APIs

Antes de provisionar compartilhamentos de arquivos ou LUNs, você deve verificar se os clusters têm máquinas virtuais de armazenamento (SVMs) criadas neles.



O fluxo de trabalho pressupõe que os clusters do ONTAP tenham sido adicionados ao Unified Manager e a chave do cluster tenha sido obtida. Os clusters devem ter as licenças necessárias para provisionar LUNs e compartilhamentos de arquivos neles.

1. Verifique se o cluster tem um SVM criado.

Categoria	Verbo HTTP	Caminho
data center	OBTER	/datacenter/svm/svms /datacenter/svm/svms/{key} }

- Onda da amostra\*

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Se a chave do SVM não for retornada, crie o SVM. Para criar os SVMs, você precisa da chave de cluster na qual você provisiona o SVM. Você também precisa especificar o nome do SVM. Siga estes passos.

Categoria	Verbo HTTP	Caminho
data center	OBTER	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}

Obtenha a chave do cluster.

- Onda da amostra\*

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

3. Na saída, obtenha a chave do cluster e, em seguida, use-a como entrada para criar o SVM.



Ao criar o SVM, garanta que ele seja compatível com todos os protocolos necessários para provisionar LUNs e compartilhamentos de arquivos neles, por exemplo, CIFS, NFS, FCP e iSCSI. Os workflows de provisionamento podem falhar se o SVM não der suporte aos serviços necessários. Recomenda-se que os serviços para os respectivos tipos de workloads também estejam habilitados no SVM.

Categoria	Verbo HTTP	Caminho
data center	POST	/datacenter/svm/svms

- Onda da amostra\*

Insira os detalhes do objeto SVM como parâmetros de entrada.

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": {}, \"key\": \"1cd8a442-86d1,type=objecttype,uuid=1cd8a442-86d1-11e0-ae1c-9876567890123\", \"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-00a0986138f7\" } ], \"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\": \"string\", \"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" }, \"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-123478563412,type=object type,uuid=1cd8a442-86d1-11e0-ae1c-9876567890123\" }, \"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ], \"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] }, \"fcg\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true, \"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" }, \"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\": \"dataLif1\" } ], \"ipspace\": { \"name\": \"exchange\" }, \"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\", \"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\", \"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ] }, \"name\": \"svm1\", \"nfs\": { \"enabled\": true }, \"nis\": { \"domain\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true }, \"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" }, \"gateway\": \"string\" } ], \"snapshot_policy\": { \"name\": \"default\" }, \"state\": \"running\", \"subtype\": \"default\" }
```

+

A saída JSON exibe uma chave de objeto Job que você pode usar para verificar o SVM que você criou.

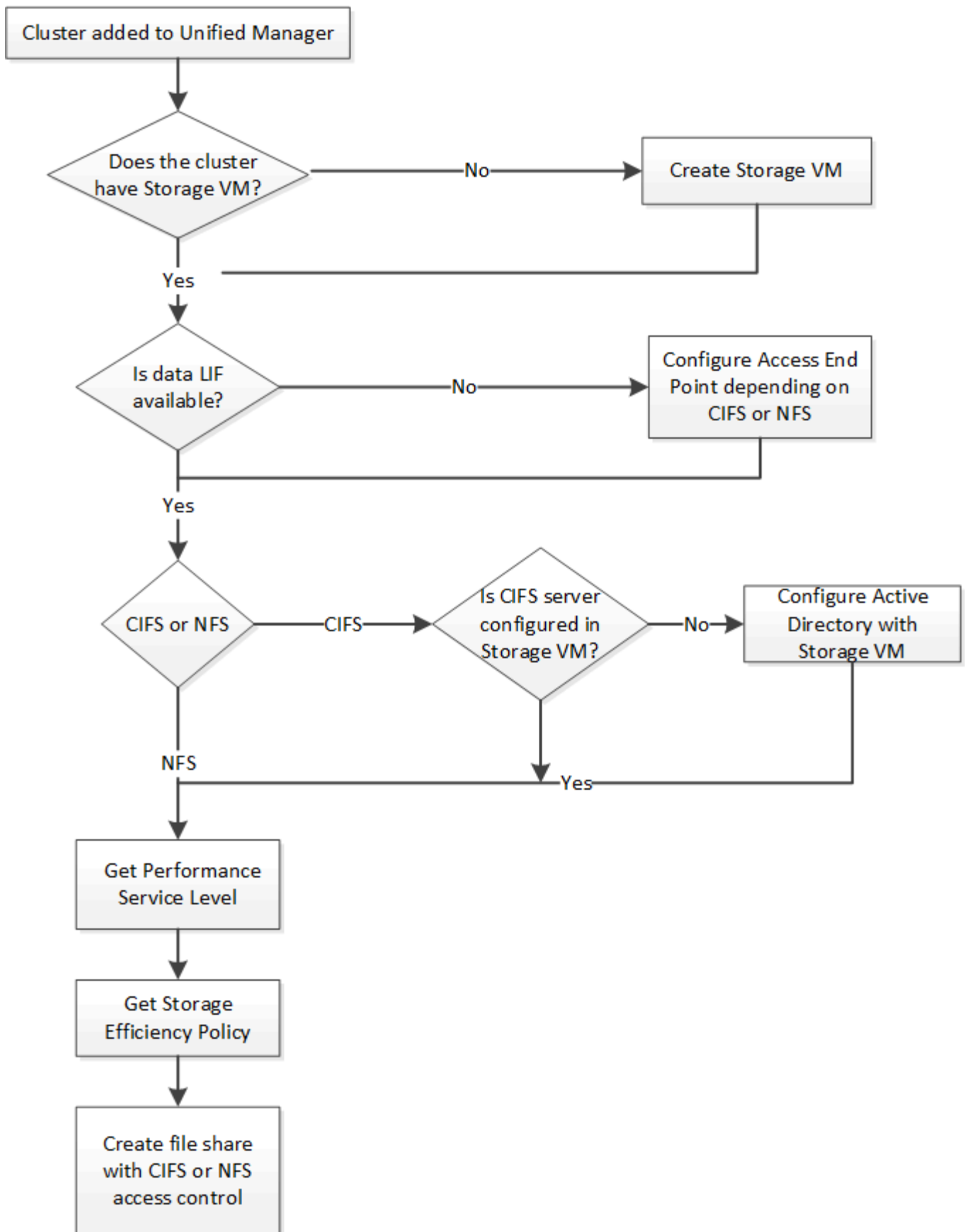
4. Verifique a criação do SVM usando a chave de objeto de tarefa para consulta. Se o SVM for criado com sucesso, a chave SVM será retornada na resposta.

Categoria	Verbo HTTP	Caminho
servidor de gerenciamento	OBTER	/management-server/jobs/{key}

## **Provisionamento de compartilhamentos de arquivos CIFS e NFS com o uso de APIs**

Você pode provisionar compartilhamentos CIFS e compartilhamentos de arquivos NFS em suas máquinas virtuais de storage (SVMs) usando as APIs de provisionamento fornecidas como parte do Active IQ Unified Manager. Esse fluxo de trabalho de provisionamento detalha as etapas para recuperar as chaves das SVMs, níveis de Serviço de Performance e políticas de eficiência de Storage antes de criar os compartilhamentos de arquivo.

O diagrama a seguir ilustra cada etapa em um fluxo de trabalho de provisionamento de compartilhamento de arquivos. Ele inclui provisionamento de compartilhamentos de arquivos CIFS e NFS.





Certifique-se de que:



- Os clusters do ONTAP foram adicionados ao Unified Manager, e a chave do cluster foi obtida.
- Os SVMs foram criados nos clusters.
- As SVMs dão suporte a serviços CIFS e NFS. O provisionamento de compartilhamentos de arquivo pode falhar se as SVMs não oferecerem suporte aos serviços necessários.
- A porta FCP está online para provisionamento de portas.

1. Determine se as LIFs de dados ou pontos de extremidade de acesso estão disponíveis no SVM no qual você deseja criar o compartilhamento CIFS. Veja a lista de pontos de extremidade de acesso disponíveis no SVM:

Categoria	Verbo HTTP	Caminho
fornecedor de storage	OBTER	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

- Onda da amostra\*

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Se o seu ponto de extremidade de acesso estiver disponível na lista, obtenha a chave de ponto de extremidade de acesso, caso contrário, crie o ponto de extremidade de acesso.



Certifique-se de criar endpoints de acesso que tenham o protocolo CIFS ativado neles. O provisionamento de compartilhamentos CIFS falha, a menos que você tenha criado um ponto de extremidade de acesso com o protocolo CIFS ativado nele.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	POST	/storage-provider/access-endpoints

- Onda da amostra\*

Você deve inserir os detalhes do endpoint de acesso que deseja criar, como parâmetros de entrada.

```
curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
\"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
\"gateway\": \"10.132.72.12\",
\"ip\": { \"address\": \"10.162.83.26\",
\"ha_address\": \"10.142.83.26\",
\"netmask\": \"255.255.0.0\" },
\"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
\"mtu\": 15000, \"name\": \"aep1\",
\"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
\"vlan\": 10}"
```

+

A saída JSON exibe uma chave de objeto Job que você pode usar para verificar o endpoint de acesso que você criou.

### 3. Verifique o ponto de extremidade de acesso:

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
servidor de gerenciamento	OBTER	/management-server/jobs/{key}

### 4. Determine se você precisa criar um compartilhamento CIFS ou um compartilhamento de arquivos NFS. Para criar compartilhamentos CIFS, siga estas subetapas:

- a. Determine se o servidor CIFS está configurado no SVM, ou seja, determinar se um mapeamento do active Directory é criado na SVM.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
fornecedor de storage	OBTER	/storage-provider/active-directories-mappings

- b. Se o mapeamento do active Directory for criado, pegue a chave; caso contrário, crie o mapeamento do active Directory na SVM.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	POST	/storage-provider/active-directories-mappings

- Onda da amostra\*

Você deve inserir os detalhes para criar o mapeamento do active Directory, como os parâmetros de entrada.

```
curl -X POST "https://<hostname>/api/storage-provider/active-directories-mappings" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \"_links\": {},
  \"dns\": \"10.000.000.000\",
  \"domain\": \"example.com\",
  \"password\": \"string\",
  \"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },
  \"username\": \"string\"}
```

+

Esta é uma chamada síncrona e você pode verificar a criação do mapeamento do active Directory na saída. Em caso de erro, a mensagem de erro é exibida para você solucionar problemas e executar novamente a solicitação.

- Obtenha a chave SVM para o SVM no qual você deseja criar o compartilhamento CIFS ou o compartilhamento de arquivos NFS, conforme descrito no tópico de fluxo de trabalho *Verificando SVMs em clusters*.
- Obtenha a chave para o nível de Serviço de desempenho executando a seguinte API e recuperando a chave da resposta.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	OBTER	/storage-provider/performance-service-levels



Você pode recuperar os detalhes dos níveis de Serviço de desempenho definidos pelo sistema, definindo o `system_defined` parâmetro de entrada como `true`. Na saída, obtenha a chave do nível de Serviço de desempenho que você deseja aplicar no compartilhamento de arquivos.

- Opcionalmente, obtenha a chave de Política de eficiência de armazenamento para a Política de eficiência de armazenamento que você deseja aplicar no compartilhamento de arquivos executando a seguinte API e recuperando a chave da resposta.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de armazenamento	OBTER	/storage-provider/storage-efficiency-policies

8. Crie o compartilhamento de arquivos. Você pode criar um compartilhamento de arquivos que suporte CIFS e NFS especificando a lista de controle de acesso e a política de exportação. As subetapas a seguir fornecem informações se você deseja criar um compartilhamento de arquivos para suportar apenas um dos protocolos no volume. Você também pode atualizar um compartilhamento de arquivos NFS para incluir a lista de controle de acesso depois de criar o compartilhamento NFS. Para obter informações, consulte o tópico *Modificação de cargas de trabalho de armazenamento*.

- a. Para criar apenas um compartilhamento CIFS, reúna as informações sobre a lista de controle de acesso (ACL). Para criar o compartilhamento CIFS, forneça valores válidos para os seguintes parâmetros de entrada. Para cada grupo de usuários que você atribuir, uma ACL é criada quando um compartilhamento CIFS/SMB é provisionado. Com base nos valores inseridos para o mapeamento ACL e ative Directory, o controle de acesso e o mapeamento são determinados para o compartilhamento CIFS quando ele é criado.

#### Um comando curl com valores de amostra

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  },
```

- b. Para criar apenas um compartilhamento de arquivos NFS, reúna as informações sobre a política de exportação. Para criar o compartilhamento de arquivos NFS, forneça valores válidos para os seguintes parâmetros de entrada. Com base em seus valores, a política de exportação é anexada ao compartilhamento de arquivos NFS quando é criada.



Ao provisionar o compartilhamento NFS, você pode criar uma política de exportação fornecendo todos os valores necessários ou fornecer a chave de política de exportação e reutilizar uma política de exportação existente. Se você quiser reutilizar uma política de exportação para a VM de armazenamento, será necessário adicionar a chave de política de exportação. A menos que você saiba a chave, você pode recuperar a chave de política de exportação usando a `/datacenter/protocols/nfs/export-policies` API. Para criar uma nova política, você deve inserir as regras conforme exibido na amostra a seguir. Para as regras inseridas, a API tenta procurar uma política de exportação existente, combinando o host, a VM de armazenamento e as regras. Se houver uma política de exportação existente, ela será usada. Caso contrário, uma nova política de exportação é criada.

### Um comando curl com valores de amostra

```
"export_policy": {
  "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
  "name_tag": "ExportPolicyNameTag",
  "rules": [
    {
      "clients": [
        {
          "match": "0.0.0.0/0"
        }
      ]
    }
  ]
}
```

Depois de configurar a lista de controle de acesso e a política de exportação, forneça os valores válidos para os parâmetros de entrada obrigatórios para compartilhamentos de arquivos CIFS e NFS:



A Política de eficiência de storage é um parâmetro opcional para a criação de compartilhamentos de arquivos.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	POST	/storage-provider/file-shares

A saída JSON exibe uma chave de objeto Job que você pode usar para verificar o compartilhamento de arquivo criado. . Verifique a criação do compartilhamento de arquivos usando a chave de objeto tarefa retornada ao consultar a tarefa:

Categoria	Verbo HTTP	Caminho
servidor de gerenciamento	OBTER	/management-server/jobs/{key}

No final da resposta, você verá a chave do compartilhamento de arquivos criada.

```

],
"job_results": [
  {
    "name": "fileshareKey",
    "value": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
  }
],
"_links": {
  "self": {
    "href": "/api/management-server/jobs/06a6148bf9e862df:-
2611856e:16e8d47e722:-7f87"
  }
}
}

```

1. Verifique a criação do compartilhamento de arquivos executando a seguinte API com a chave retornada:

Categoria	Verbo HTTP	Caminho
fornecedor de storage	OBTER	/storage-provider/file-shares/{key}

◦ Amostra de saída JSON\*

Você pode ver que o método POST de /storage-provider/file-shares internamente invoca todas as APIs necessárias para cada uma das funções e cria o objeto. Por exemplo, ele invoca a /storage-provider/performance-service-levels/ API para atribuir o nível de Serviço de desempenho no compartilhamento de arquivos.

```

{
  "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
  "name": "FileShare_377",
  "cluster": {
    "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
    "name": "AFFA300-206-68-70-72-74",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-
00a098dcc959"
      }
    }
  }
}

```

```

    },
    "svm": {
      "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
      "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
      "name": "RRT_ritu_vs1",
      "_links": {
        "self": {
          "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959"
        }
      }
    },
    "assigned_performance_service_level": {
      "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
      "name": "Value",
      "peak_iops": 75,
      "expected_iops": 75,
      "_links": {
        "self": {
          "href": "/api/storage-provider/performance-service-levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
        }
      }
    },
    "recommended_performance_service_level": {
      "key": null,
      "name": "Idle",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
    "space": {
      "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
      "key": null,
      "name": "Unassigned",
      "_links": {}
    },
    "access_control": {
      "acl": [
        {
          "user_or_group": "everyone",

```

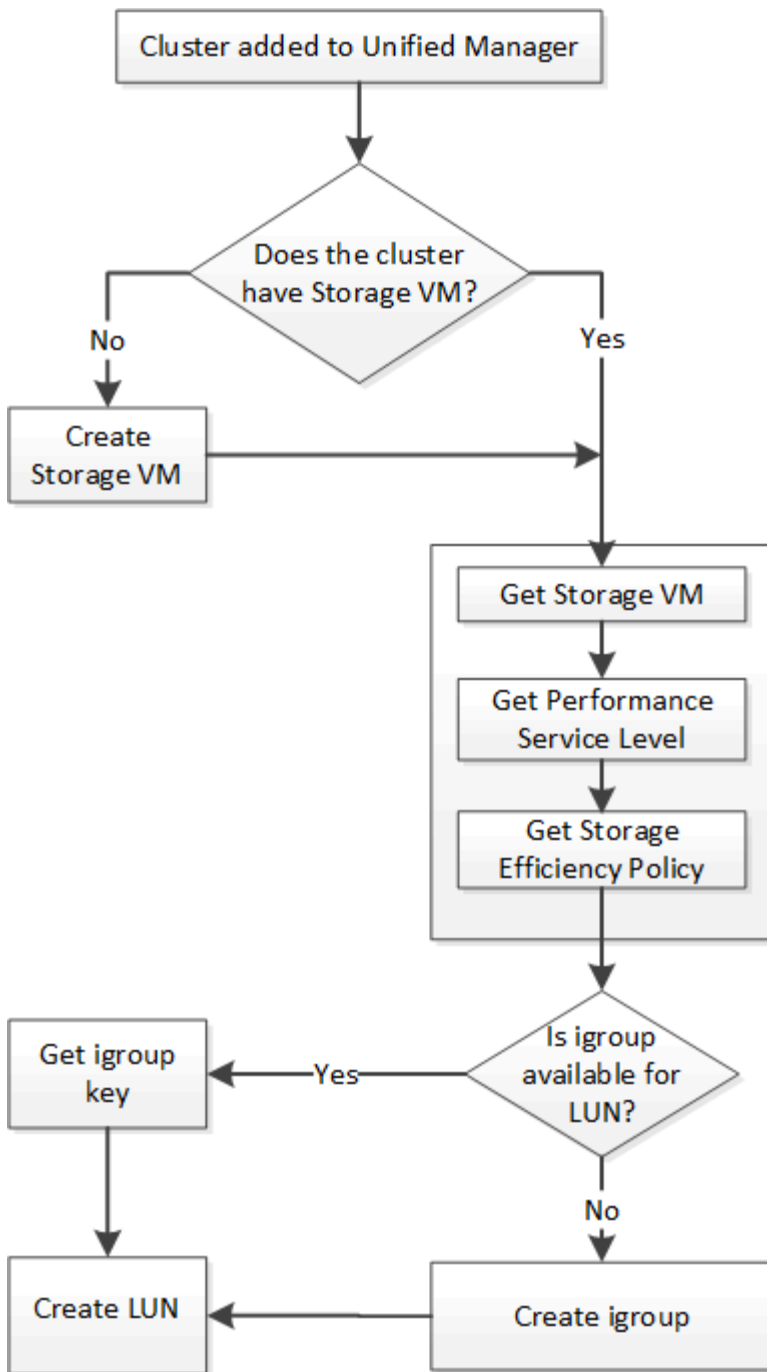
```

        "permission": "read"
    }
],
"export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
        {
            "anonymous_user": "65534",
            "clients": [
                {
                    "match": "0.0.0.0/0"
                }
            ],
            "index": 1,
            "protocols": [
                "nfs3",
                "nfs4"
            ],
            "ro_rule": [
                "sys"
            ],
            "rw_rule": [
                "sys"
            ],
            "superuser": [
                "none"
            ]
        },
        {
            "anonymous_user": "65534",
            "clients": [
                {
                    "match": "0.0.0.0/0"
                }
            ],
            "index": 2,
            "protocols": [
                "cifs"
            ],
            "ro_rule": [
                "ntlm"
            ],
            "rw_rule": [

```







Esse fluxo de trabalho pressupõe que os clusters do ONTAP tenham sido adicionados ao Unified Manager e que a chave do cluster tenha sido obtida. O fluxo de trabalho também pressupõe que os SVMs já foram criados nos clusters.

1. Obtenha a chave SVM para o SVM no qual você deseja criar o LUN, conforme descrito no tópico *Verificando SVMs em clusters* fluxo de trabalho.
2. Obtenha a chave para o nível de Serviço de desempenho executando a seguinte API e recuperando a chave da resposta.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de armazenamento	GET	/storage-provider/performance-service-levels



Você pode recuperar os detalhes dos níveis de Serviço de desempenho definidos pelo sistema, definindo o `system_defined` parâmetro de entrada como `true`. A partir da saída, obtenha a chave do nível de Serviço de desempenho que você deseja aplicar no LUN.

3. Opcionalmente, obtenha a chave de Política de eficiência de armazenamento para a Política de eficiência de armazenamento que você deseja aplicar no LUN executando a seguinte API e recuperando a chave da resposta.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
provedor de armazenamento	GET	/storage-provider/storage-efficiency-policies

4. Determine se grupos de iniciadores (grupos de iniciadores) foram criados para conceder acesso ao destino LUN que você deseja criar.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
data center	GET	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}

Você deve inserir o valor do parâmetro para indicar o SVM para o qual o igroup tem acesso autorizado. Além disso, se você quiser consultar um determinado grupo, digite o nome do grupo (chave) como um parâmetro de entrada.

5. Na saída, se você puder encontrar o igroup ao qual deseja conceder acesso, obtenha a chave. Caso contrário, crie o grupo.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
data center	POST	/datacenter/protocols/san/igroups

Você deve inserir os detalhes do grupo que deseja criar, como os parâmetros de entrada. Esta é uma chamada síncrona e você pode verificar a criação do igroup na saída. Em caso de erro, uma mensagem é exibida para você solucionar problemas e executar novamente a API.

6. Crie o LUN.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
fornecedor de storage	POST	/storage-provider/luns

Para criar o LUN, certifique-se de que adicionou os valores recuperados como parâmetros de entrada obrigatórios.



A Política de eficiência de storage é um parâmetro opcional para a criação de LUNs.

- Onda da amostra\*

Tem de introduzir todos os detalhes do LUN que pretende criar, como parâmetros de entrada.

A saída JSON exibe uma chave de objeto Job que você pode usar para verificar o LUN que você criou.

7. Verifique a criação de LUN usando a chave de objeto Job retornada ao consultar a tarefa:

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
servidor de gerenciamento	OBTER	/management-server/jobs/{key}

No final da resposta, você verá a chave do LUN criada.

8. Verifique a criação do LUN executando a seguinte API com a chave retornada:

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
fornecedor de storage	OBTER	/storage-provider/luns/{key}

- Amostra de saída JSON\*

Você pode ver que o método POST de /storage-provider/luns internamente invoca todas as APIs necessárias para cada uma das funções e cria o objeto. Por exemplo, ele invoca a /storage-provider/performance-service-levels/ API para atribuir o nível de Serviço de desempenho no LUN.

Etapas de solução de problemas para falha na criação ou mapeamento de LUN

Ao concluir esse fluxo de trabalho, você ainda poderá ver uma falha na criação de LUN. Mesmo que o LUN seja criado com sucesso, o mapeamento LUN com o igroup pode falhar devido à indisponibilidade de um LIF SAN ou ponto de extremidade de acesso no nó em que você cria o LUN. Em caso de falha, você pode ver a seguinte mensagem:

```
The nodes <node_name> and <partner_node_name> have no LIFs configured with the iSCSI or FCP protocol for Vserver <server_name>. Use the access-endpoints API to create a LIF for the LUN.
```

Siga estas etapas de solução de problemas para contornar essa falha.

1. Crie um ponto de extremidade de acesso compatível com o protocolo iSCSI/FCP no SVM no qual você tentou criar o LUN.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
fornecedor de storage	POST	/storage-provider/access-endpoints

- Onda da amostra\*

Você deve inserir os detalhes do endpoint de acesso que deseja criar, como os parâmetros de entrada.



Certifique-se de que no parâmetro de entrada você adicionou o endereço para indicar o nó inicial do LUN e o `ha_address` para indicar o nó do parceiro do nó inicial. Quando você executa essa operação, ela cria pontos de extremidade de acesso no nó inicial e no nó do parceiro.

2. Consulte a tarefa com a chave de objeto Job retornada na saída JSON para verificar se ela foi executada com sucesso para adicionar os pontos de extremidade de acesso à SVM e se os serviços iSCSI/FCP foram ativados na SVM.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
servidor de gerenciamento	OBTER	/management-server/jobs/{key}

- Amostra de saída JSON\*

No final da saída, você pode ver a chave dos endpoints de acesso criados. Na saída a seguir, o valor "name": "AccessEndpointKey" indica o ponto final de acesso criado no nó inicial do LUN, para o qual a chave é 9c964258-14ef-11ea-95e2-00a098e32c28. O valor "nome": "AccessEndpointHAKey" indica o ponto de extremidade de acesso criado no nó de parceiro do nó inicial, para o qual a chave é 9d347006-14ef-11ea-8760-00a098e3215f.

3. Modifique o LUN para atualizar o mapeamento do igrop. Para obter mais informações sobre a modificação do fluxo de trabalho, consulte ""Modificação de cargas de trabalho de armazenamento"".

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
fornecedor de storage	PATCH	/storage-provider/lun/{key}

Na entrada, especifique a chave igrop com a qual você deseja atualizar o mapeamento LUN, juntamente com a chave LUN.

- Onda da amostra\*

A saída JSON exibe uma chave de objeto Job que você pode usar para verificar se o mapeamento foi bem-sucedido.

4. Verifique o mapeamento LUN consultando a chave LUN.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	OBTER	/storage-provider/luns/{key}

- Amostra de saída JSON\*

Na saída, você pode ver que o LUN foi mapeado com sucesso com o igroup (chave d19ec2fa-fec7-11e8-B23D-00a098e32c28) com o qual foi inicialmente provisionado.

### Como modificar workloads de storage usando APIs

A modificação de workloads de storage consiste na atualização de LUNs ou compartilhamentos de arquivos com parâmetros ausentes ou na alteração dos parâmetros existentes.

Esse fluxo de trabalho toma o exemplo de atualização dos níveis de Serviço de Performance para LUNs e compartilhamentos de arquivos.



O fluxo de trabalho pressupõe que o LUN ou o compartilhamento de arquivos tenha sido provisionado com níveis de Serviço de Performance.

### Modificação de compartilhamentos de arquivo

Ao modificar um compartilhamento de arquivos, você pode atualizar os seguintes parâmetros:

- Capacidade ou tamanho.
- Configuração online ou offline.
- Política de eficiência de storage.
- Nível de Serviço de desempenho.
- Definições da lista de controlo de acesso (ACL).
- Exportar definições de política. Você também pode excluir parâmetros de política de exportação e reverter as regras de política de exportação padrão (vazias) no compartilhamento de arquivos.



Durante uma única execução de API, você pode atualizar apenas um parâmetro.

Este procedimento descreve a adição de um nível de Serviço de desempenho a um compartilhamento de arquivos. Você pode usar o mesmo procedimento para atualizar qualquer outra propriedade de compartilhamento de arquivos.

1. Obtenha a chave de compartilhamento de arquivos CIFS ou NFS do compartilhamento de arquivos que você deseja atualizar. Essa API consulta todos os compartilhamentos de arquivo no data center. Ignore esta etapa se você já souber a chave de compartilhamento de arquivos.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
fornecedor de storage	OBTER	/storage-provider/file-shares

2. Veja os detalhes do compartilhamento de arquivos executando a seguinte API com a chave de compartilhamento de arquivos obtida.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
fornecedor de storage	OBTER	/storage-provider/file-shares/{key}

Veja os detalhes do compartilhamento de arquivo na saída.

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

3. Obtenha a chave para o nível de Serviço de desempenho que você deseja atribuir neste compartilhamento de arquivos. Atualmente, nenhuma política está atribuída a ela.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
Níveis de serviço de performance	OBTER	/storage-provider/performance-service-levels



Você pode recuperar os detalhes dos níveis de Serviço de desempenho definidos pelo sistema, definindo o `system_defined` parâmetro de entrada como `true`. Na saída, obtenha a chave do nível de Serviço de desempenho que você deseja aplicar ao compartilhamento de arquivos.

4. Aplique o nível de Serviço de desempenho no compartilhamento de arquivos.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
Fornecedor de armazenamento	PATCH	/storage-provider/file-shares/{key}

Na entrada, você deve especificar apenas o parâmetro que deseja atualizar, juntamente com a chave de compartilhamento de arquivos. Neste caso, é a chave do nível de Serviço de desempenho.

◦ Onda da amostra\*

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
  \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

+

A saída JSON exibe um objeto Job que você pode usar para verificar se os pontos de extremidade de acesso nos nós de casa e parceiros foram criados com sucesso.

5. Verifique se o nível de Serviço de desempenho foi adicionado ao compartilhamento de arquivos usando a chave de objeto trabalho exibida na saída.

Categoria	Verbo HTTP	Caminho
Servidor de gerenciamento	OBTER	/management-server/jobs/{key}

Se você consultar pelo ID do objeto Job, verá se o compartilhamento de arquivo foi atualizado com êxito. Em caso de falha, solucione a falha e execute a API novamente. Na criação bem-sucedida, consulte o compartilhamento de arquivos para ver o objeto modificado:

Categoria	Verbo HTTP	Caminho
fornecedor de storage	OBTER	/storage-provider/file-shares/{key}

Veja os detalhes do compartilhamento de arquivo na saída.

```
"assigned_performance_service_level": {
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
  "name": "Value",
  "peak_iops": 75,
  "expected_iops": 75,
  "_links": {
    "self": {
      "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
    }
  }
}
```



## A atualizar LUNs

Durante a atualização de um LUN, você pode modificar os seguintes parâmetros:

- Capacidade ou tamanho
- Configuração online ou offline
- Política de eficiência de storage
- Nível de Serviço de desempenho
- Mapa de LUN



Durante uma única execução de API, você pode atualizar apenas um parâmetro.

Este procedimento descreve a adição de um nível de Serviço de desempenho a um LUN. Você pode usar o mesmo procedimento para atualizar qualquer outra propriedade LUN.

1. Obtenha a chave LUN do LUN que pretende atualizar. Essa API retorna detalhes de todos OS LUNS no data center. Ignore esta etapa se você já souber a chave LUN.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
Fornecedor de armazenamento	OBTER	/storage-provider/luns

2. Veja os detalhes do LUN executando a seguinte API com a chave LUN que você obteve.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
Fornecedor de armazenamento	OBTER	/storage-provider/luns/{key}

Veja os detalhes do LUN na saída. Você pode ver que não há nenhum nível de Serviço de desempenho atribuído a este LUN.

- Amostra de saída JSON\*

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

3. Obtenha a chave para o nível de Serviço de desempenho que você deseja atribuir ao LUN.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
Níveis de serviço de performance	OBTER	/storage-provider/performance-service-levels



Você pode recuperar os detalhes dos níveis de Serviço de desempenho definidos pelo sistema, definindo o `system_defined` parâmetro de entrada como `true`. A partir da saída, obtenha a chave do nível de Serviço de desempenho que você deseja aplicar no LUN.

#### 4. Aplique o nível de Serviço de desempenho no LUN.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
Fornecedor de armazenamento	PATCH	/storage-provider/lun/{key}

Na entrada, você deve especificar apenas o parâmetro que deseja atualizar, juntamente com a chave LUN. Neste caso, é a chave do nível de Serviço de desempenho.

- Onda da amostra\*

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" -d "{ \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-fa163e82bbf2\" } }"
```

+

A saída JSON exibe uma chave de objeto Job que você pode usar para verificar o LUN que você atualizou.

#### 5. Veja os detalhes do LUN executando a seguinte API com a chave LUN que você obteve.

<b>Categoria</b>	<b>Verbo HTTP</b>	<b>Caminho</b>
Fornecedor de armazenamento	OBTER	/storage-provider/luns/{key}

Veja os detalhes do LUN na saída. Pode ver que o nível de Serviço de desempenho está atribuído a este LUN.

- Amostra de saída JSON\*

```

"assigned_performance_service_level": {
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
  "name": "Value",
  "peak_iops": 75,
  "expected_iops": 75,
  "_links": {
    "self": {
      "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
    }
  }
}

```

## Modificação de um compartilhamento de arquivos NFS usando APIs para oferecer suporte a CIFS

Você pode modificar um compartilhamento de arquivos NFS para dar suporte ao protocolo CIFS. Durante a criação do compartilhamento de arquivos, é possível especificar os parâmetros da lista de controle de acesso (ACL) e as regras de política de exportação para o mesmo compartilhamento de arquivos. No entanto, se quiser ativar o CIFS no mesmo volume em que criou um compartilhamento de arquivos NFS, você pode atualizar os parâmetros ACL nesse compartilhamento de arquivos para oferecer suporte ao CIFS.

### Antes de começar

1. Um compartilhamento de arquivos NFS deve ter sido criado apenas com os detalhes da política de exportação. Para obter informações, consulte *Gerenciando compartilhamentos de arquivos e modificando cargas de trabalho de armazenamento*.
2. Você deve ter a chave de compartilhamento de arquivos para executar esta operação. Para obter informações sobre como visualizar detalhes do compartilhamento de arquivos e recuperar a chave de compartilhamento de arquivos usando o ID da tarefa, consulte *Provisioning CIFS e compartilhamentos de arquivos NFS*.

Isso é aplicável a um compartilhamento de arquivos NFS que você criou adicionando apenas regras de política de exportação e não parâmetros ACL. Você modifica o compartilhamento de arquivos NFS para incluir os parâmetros ACL.

### Passos

1. No compartilhamento de arquivos NFS, execute uma PATCH operação com os detalhes da ACL para permitir o acesso CIFS.

Categoria	Verbo HTTP	Caminho
fornecedor de storage	PATCH	/storage-provider/file-shares

- Onda da amostra\*

Com base no Access Privileges que você atribui ao grupo de usuários, conforme exibido na amostra a seguir, uma ACL é criada e atribuída ao compartilhamento de arquivos.

```

{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  }
}

```

◦ Amostra de saída JSON\*

A operação retorna o ID do trabalho do trabalho que executa a atualização.

2. Verifique se os parâmetros foram adicionados corretamente consultando os detalhes do compartilhamento de arquivo para o mesmo compartilhamento de arquivo.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	/storage-provider/file-shares/{key}

◦ Amostra de saída JSON\*

```

"access_control": {
  "acl": [
    {
      "user_or_group": "everyone",
      "permission": "read"
    }
  ],
  "export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ]
      }
    ],
  }
}

```

```

        "index": 1,
        "protocols": [
            "nfs3",
            "nfs4"
        ],
        "ro_rule": [
            "sys"
        ],
        "rw_rule": [
            "sys"
        ],
        "superuser": [
            "none"
        ]
    },
    {
        "anonymous_user": "65534",
        "clients": [
            {
                "match": "0.0.0.0/0"
            }
        ],
        "index": 2,
        "protocols": [
            "cifs"
        ],
        "ro_rule": [
            "ntlm"
        ],
        "rw_rule": [
            "ntlm"
        ],
        "superuser": [
            "none"
        ]
    }
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
},

```

```
  "_links": {
    "self": {
      "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
    }
  }
}
```

+

Você pode ver a ACL atribuída juntamente com a política de exportação para o mesmo compartilhamento de arquivos.

# Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

## Direitos de autor

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Política de privacidade

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Código aberto

Informações sobre direitos autorais de terceiros e licenças usadas neste produto.

["Aviso para Active IQ Unified Manager 9,16"](#)

## Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.