



Documentação do Active IQ Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

This PDF was generated from <https://docs.netapp.com/pt-br/active-iq-unified-manager-916/index.html> on October 15, 2025. Always check docs.netapp.com for the latest.

Índice

Documentação do Active IQ Unified Manager	1
Notas de lançamento	2
Começar	3
Instruções de início rápido para instalações do VMware	3
Requisitos do sistema	3
Instalar o Active IQ Unified Manager	3
Instruções de início rápido para instalações Linux	4
Requisitos do sistema	4
Instalar o Active IQ Unified Manager	4
Instruções de início rápido para instalações do Windows	5
Requisitos do sistema	5
Instalar o Active IQ Unified Manager	6
Instalar o Unified Manager em sistemas VMware vSphere	7
Introdução ao Active IQ Unified Manager	7
O que o servidor Unified Manager faz	7
Visão geral da sequência de instalação	7
Requisitos para instalar o Unified Manager	8
Requisitos de infraestrutura virtual e sistema de hardware	8
Requisitos de instalação e software VMware	9
Navegadores suportados	10
Requisitos de protocolo e porta	11
Complete a planilha	14
Instalar, atualizar e remover o software Unified Manager	16
Visão geral do processo de implantação	16
Implantar o Unified Manager	17
Atualizar o Unified Manager	21
Reinicie a máquina virtual do Unified Manager	24
Remover o Unified Manager	24
Instalar o Unified Manager em sistemas Linux	25
Introdução ao Active IQ Unified Manager	25
O que o servidor Unified Manager faz	25
Visão geral da sequência de instalação	25
Requisitos para instalar o Unified Manager	26
Requisitos de infraestrutura virtual e sistema de hardware	26
Requisitos de instalação e software Linux	28
Navegadores suportados	30
Requisitos de protocolo e porta	31
Complete a planilha	34
Instalar, atualizar e remover o software Unified Manager	36
Visão geral do processo de instalação	36
Configurar repositórios de software necessários	37
Requisitos do SELinux em compartilhamentos NFS e CIFS	38
Instalar o Unified Manager em sistemas Linux	41

Atualizar o Unified Manager no Red Hat Enterprise Linux	48
Atualizar produtos de terceiros após a instalação do Unified Manager	53
Reiniciar o Unified Manager	54
Remover o Unified Manager	54
Remover o usuário umadmin personalizado e o grupo de manutenção	55
Instalar o Unified Manager em sistemas Windows	56
Introdução ao Active IQ Unified Manager	56
O que o servidor Unified Manager faz	56
Visão geral da sequência de instalação	56
Requisitos para instalar o Unified Manager	57
Requisitos de infraestrutura virtual e sistema de hardware	57
Requisitos de software e instalação do Windows	59
Navegadores suportados	60
Requisitos de protocolo e porta	61
Complete a planilha	64
Instalar, atualizar e remover o software Unified Manager	66
Visão geral do processo de instalação	66
Instalar o Unified Manager no Windows	67
Alterar a senha do JBoss	70
Caminho de atualização com suporte para versões do Unified Manager	71
Atualizar o Unified Manager	71
Atualizar produtos de terceiros	73
Desinstalar produtos de terceiros	74
Reiniciar o Unified Manager	74
Desinstalar o Unified Manager	75
Executar tarefas de configuração e administrativas	77
Configurar o Active IQ Unified Manager	77
Visão geral da sequência de configuração	77
Acesse a interface da Web do Unified Manager	77
Execute a configuração inicial da interface da Web do Unified Manager	78
Adicionar clusters	80
Configurar o Unified Manager para enviar notificações de alerta	82
Alterar a senha do usuário local	91
Definir o tempo limite de inatividade da sessão	91
Defina o tempo limite da sessão por meio da CLI	92
Alterar o nome do host do Unified Manager	92
Habilitar e desabilitar o gerenciamento de armazenamento baseado em políticas	97
Configurar backup do Unified Manager	98
Gerenciar configurações de recursos	98
Habilitar gerenciamento de armazenamento baseado em políticas	99
Habilitar API Gateway	99
Especificar tempo limite de inatividade	100
Habilitar eventos do portal Active IQ	100
Habilitar e desabilitar configurações de segurança para conformidade	101
Habilitar e desabilitar upload de scripts	102

Adicionar banner de login	102
Use o console de manutenção	102
Que funcionalidade o console de manutenção fornece	102
O que o usuário de manutenção faz	103
Capacidades de diagnóstico do usuário	103
Acesse o console de manutenção	103
Acesse o console de manutenção usando o console da VM do vSphere	104
Menus do console de manutenção	105
Alterar a senha do usuário de manutenção no Windows	110
Alterar a senha do umadmin em sistemas Linux	110
Alterar as portas que o Unified Manager usa para os protocolos HTTP e HTTPS	111
Adicionar interfaces de rede	111
Adicionar espaço em disco ao diretório do banco de dados do Unified Manager	112
Gerenciar acesso do usuário	116
Adicionar usuários	116
Editar as configurações do usuário	117
Ver usuários	118
Excluir usuários ou grupos	118
O que é RBAC	118
O que o controle de acesso baseado em função faz	119
Definições de tipos de usuários	119
Definições de funções de usuário	120
Funções e recursos do usuário do Unified Manager	121
Gerenciar configurações de autenticação SAML	123
Requisitos do provedor de identidade	123
Habilitar autenticação SAML	124
Alterar o provedor de identidade usado para autenticação SAML	125
Atualizar as configurações de autenticação SAML após a alteração do certificado de segurança do Unified Manager	126
Desativar autenticação SAML	127
Desabilitar a autenticação SAML no console de manutenção	128
Página de autenticação SAML	129
Gerenciar autenticação	129
Editar servidores de autenticação	130
Excluir servidores de autenticação	130
Autenticação com Active Directory ou OpenLDAP	130
Registro de auditoria	131
Página de autenticação remota	134
Gerenciar certificados de segurança	137
Visualizar o certificado de segurança HTTPS	137
Baixe uma solicitação de assinatura de certificado HTTPS	137
Instalar um certificado HTTPS assinado e retornado pela CA	138
Instalar um certificado HTTPS gerado usando ferramentas externas	139
Descrições de páginas para gerenciamento de certificados	141
Monitorar e gerenciar armazenamento	144

Introdução ao Active IQ Unified Manager	144
Introdução ao monitoramento de integridade do Active IQ Unified Manager	144
Introdução ao monitoramento de desempenho do Active IQ Unified Manager	145
Usar APIs REST do Unified Manager	146
O que o servidor Unified Manager faz	146
Entenda a interface do usuário	147
Layouts típicos de janelas	147
Personalização do layout da janela	148
Use a Ajuda do Unified Manager	149
Marque seus tópicos de ajuda favoritos	150
Pesquisar objetos de armazenamento	150
Exportar dados de armazenamento como relatórios	151
Filtrar conteúdo da página de inventário	152
Visualizar eventos ativos no sino de notificação	154
Monitore e gerencie clusters no painel	154
Página do painel	155
Gerencie problemas ou recursos do ONTAP diretamente do Unified Manager	158
Gerenciar clusters	166
Como funciona o processo de descoberta de cluster	166
Ver a lista de clusters monitorados	167
Adicionar clusters	167
Editar clusters	170
Remover clusters	170
Redescubra clusters	171
Monitorar a infraestrutura virtual VMware	171
O que não é suportado	174
Visualizar e adicionar o vCenter Server	175
Remover o vCenter Server	177
Monitorar máquinas virtuais	177
Visualizar infraestrutura virtual em uma configuração de recuperação de desastres	179
Provisionar e gerenciar cargas de trabalho	181
Visão geral das cargas de trabalho	182
Níveis de serviço de desempenho	189
Gerenciar políticas de eficiência de armazenamento	196
Gerenciar e monitorar configurações do MetroCluster	198
Comportamento do volume durante a comutação e o retorno	199
Definições de status de conectividade de cluster para configuração do MetroCluster sobre FC	201
Definições de status de espelhamento de dados para MetroCluster sobre FC	202
Monitorar configurações do MetroCluster	202
Monitorar a replicação do MetroCluster	205
Gerenciar cotas	206
Quais são os limites de cota	206
Exibir cotas de usuários e grupos de usuários	206
Crie regras para gerar endereços de e-mail	207
Crie um formato de notificação por e-mail para cotas de usuários e grupos de usuários	207

Editar endereços de e-mail de cotas de usuários e grupos	208
Entenda mais sobre cotas	209
Descrição das caixas de diálogo de cotas	210
Solução de problemas	213
Adicionar espaço em disco ao diretório do banco de dados do Unified Manager	213
Alterar o intervalo de coleta de estatísticas de desempenho	216
Alterar o período de tempo em que o Unified Manager retém dados de eventos e desempenho	217
Erro de autenticação desconhecido	218
Usuário não encontrado	219
Problema ao adicionar LDAP usando outros serviços de autenticação	219
Problema de rotação de log do NetApp Manageability SDK em sistemas Windows	220
Gerenciar eventos e alertas	221
Gerenciar eventos	221
O que são os eventos da plataforma Active IQ	221
O que são eventos do Sistema de Gerenciamento de Eventos	221
O que acontece quando um evento é recebido	227
Ver eventos e detalhes dos eventos	228
Ver eventos não atribuídos	229
Reconhecer e resolver eventos	229
Atribuir eventos a usuários específicos	230
Desativar eventos indesejados	231
Corrigir problemas usando a correção automática do Unified Manager	232
Habilitar e desabilitar relatórios de eventos do Active IQ	233
Carregar um novo arquivo de regras do Active IQ	234
Como os eventos da plataforma Active IQ são gerados	235
Resolver eventos da plataforma Active IQ	235
Configurar definições de retenção de eventos	236
O que é uma janela de manutenção do Unified Manager	236
Gerenciar eventos de recursos do sistema host	239
Entenda mais sobre os eventos	239
Lista de eventos e tipos de gravidade	245
Descrição das janelas de eventos e caixas de diálogo	306
Gerenciar alertas	319
O que são alertas	319
Quais informações estão contidas em um e-mail de alerta	319
Adicionar alertas	320
Adicionar alertas para eventos de desempenho	323
Alertas de teste	324
Habilitar e desabilitar alertas para eventos Resolvidos e Obsoletos	324
Excluir volumes de destino de recuperação de desastres da geração de alertas	325
Ver alertas	326
Editar alertas	326
Excluir alertas	326
Descrição das janelas de alerta e caixas de diálogo	327
Gerenciar scripts	333

Como os scripts funcionam com alertas	333
Adicionar scripts	334
Excluir scripts	335
Execução do script de teste	335
Comandos CLI do Unified Manager suportados	336
Descrição das janelas de script e caixas de diálogo	342
Monitorar e gerenciar o desempenho do cluster	344
Introdução ao monitoramento de desempenho do Active IQ Unified Manager	344
Recursos de monitoramento de desempenho do Unified Manager	344
Interfaces do Unified Manager usadas para gerenciar o desempenho do sistema de armazenamento	345
Configuração de cluster e atividade de coleta de dados de desempenho	345
O que é um ciclo de coleta de continuidade de dados	347
O que o registro de data e hora significa em dados e eventos coletados	348
Navegue pelos fluxos de trabalho de desempenho na GUI do Unified Manager	348
Efetue login na interface do usuário	348
Interface gráfica e caminhos de navegação	349
Pesquisar objetos de armazenamento	354
Filtrar conteúdo da página de inventário	355
Monitore o desempenho do cluster no Painel	357
Entenda os painéis de desempenho no Dashboard	357
Mensagens e descrições de banners de desempenho	358
Alterar o intervalo de coleta de estatísticas de desempenho	358
Solucionar problemas de cargas de trabalho usando o analisador de carga de trabalho	359
Quais dados o analisador de carga de trabalho exibe	360
Quando devo usar o analisador de carga de trabalho	361
Use o analisador de carga de trabalho	362
Monitore o desempenho do cluster na página inicial do Performance Cluster	362
Entenda a página de destino do cluster de desempenho	363
Página de destino do cluster de desempenho	363
Monitore o desempenho usando as páginas do Inventário de Desempenho	368
Exibir páginas de inventário de desempenho para todos os objetos de armazenamento	369
Refinando o conteúdo da página de inventário de desempenho	374
Entenda as recomendações do Unified Manager para hierarquizar dados na nuvem	377
Monitore o desempenho usando as páginas do Performance Explorer	378
Entenda o objeto raiz	379
Aplique filtragem para reduzir a lista de objetos correlacionados na grade	379
Especifique um intervalo de tempo para objetos correlacionados	379
Defina a lista de objetos correlacionados para gráficos de comparação	381
Entenda os gráficos de contador	382
Tipos de gráficos de contador de desempenho	383
Selecione gráficos de desempenho para exibir	386
Expandir o painel Gráficos de Contadores	386
Alterar o foco dos gráficos de contador para um período de tempo mais curto	387
Ver detalhes do evento na Linha do tempo de eventos	387
Visualização de zoom de gráficos de contador	388

Exibir latência de volume por componente do cluster	391
Visualizar tráfego SVM IOPS por protocolo	391
Visualize gráficos de volume e latência de LUN para verificar a garantia de desempenho	392
Veja o desempenho de todos os clusters do SAN Array	392
Exibir IOPS do nó com base em cargas de trabalho que residem apenas no nó local	393
Componentes das páginas de destino do objeto	394
Gerenciar desempenho usando informações do grupo de políticas de QoS	400
Como o QoS de armazenamento pode controlar a taxa de transferência da carga de trabalho	400
Exibir todos os grupos de políticas de QoS disponíveis em todos os clusters	401
Exibir volumes ou LUNs que estão no mesmo grupo de política de QoS	402
Visualize as configurações do grupo de políticas de QoS aplicadas a volumes ou LUNs específicos ..	403
Visualize gráficos de desempenho para comparar volumes ou LUNs que estão no mesmo grupo de políticas de QoS	403
Como diferentes tipos de políticas de QoS são exibidos nos gráficos de taxa de transferência	404
Visualize as configurações mínimas e máximas de QoS da carga de trabalho no Performance Explorer	405
Gerencie o desempenho usando a capacidade de desempenho e as informações de IOPS disponíveis ..	406
Qual é a capacidade de desempenho utilizada	407
O que significa o valor da capacidade de desempenho utilizada	408
O que é IOPS disponível	409
Exibir valores usados de capacidade de desempenho de nó e agregado	410
Exibir valores de IOPS disponíveis para nós e agregados	411
Visualize gráficos de contadores de capacidade de desempenho para identificar problemas	412
Capacidade de desempenho usada em condições de limiar de desempenho	414
Use o contador de capacidade de desempenho usado para gerenciar o desempenho	415
Entenda e use a página de planejamento de failover de nó	416
Use a página Planejamento de Failover de Nó para determinar ações corretivas	416
Componentes da página de planejamento de failover de nó	416
Use uma política de limite com a página Planejamento de Failover de Nó	418
Use o gráfico de detalhamento da capacidade de desempenho usada para planejamento de failover ..	418
Coletar dados e monitorar o desempenho da carga de trabalho	420
Tipos de cargas de trabalho monitoradas pelo Unified Manager	420
Valores de medição de desempenho da carga de trabalho	421
Qual é a faixa de desempenho esperada	423
Como a previsão de latência é usada na análise de desempenho	424
Como o Unified Manager usa a latência da carga de trabalho para identificar problemas de desempenho	425
Como as operações de cluster podem afetar a latência da carga de trabalho	426
Monitoramento de desempenho das configurações do MetroCluster	427
Entenda eventos de desempenho e alertas	428
Fontes de eventos de desempenho	428
Tipos de gravidade de eventos de desempenho	429
Alterações de configuração detectadas pelo Unified Manager	430
Tipos de políticas de limite de desempenho definidas pelo sistema	430
Análise e notificação de eventos de desempenho	433

Como o Unified Manager determina o impacto no desempenho de um evento	435
Componentes do cluster e por que eles podem estar em disputa	436
Funções das cargas de trabalho envolvidas em um evento de desempenho	438
Gerenciar limites de desempenho	439
Como funcionam as políticas de limite de desempenho definidas pelo usuário	439
O que acontece quando uma política de limite de desempenho é violada	441
Quais contadores de desempenho podem ser rastreados usando limites	441
Quais objetos e contadores podem ser usados em políticas de limite de combinação	444
Crie políticas de limite de desempenho definidas pelo usuário	444
Atribuir políticas de limite de desempenho a objetos de armazenamento	446
Ver políticas de limite de desempenho	447
Editar políticas de limite de desempenho definidas pelo usuário	447
Remover políticas de limite de desempenho de objetos de armazenamento	448
O que acontece quando uma política de limite de desempenho é alterada	449
O que acontece com as políticas de limite de desempenho quando um objeto é movido	449
Analisar eventos de desempenho	450
Exibir informações sobre eventos de desempenho	450
Analisar eventos a partir de limites de desempenho definidos pelo usuário	451
Analisar eventos a partir de limites de desempenho definidos pelo sistema	452
Analisar eventos a partir de limites de desempenho dinâmico	458
Resolver eventos de desempenho	466
Confirme se a latência está dentro do intervalo esperado	466
Analise o impacto das alterações de configuração no desempenho da carga de trabalho	466
Opções para melhorar o desempenho da carga de trabalho do lado do cliente	466
Verifique se há problemas de cliente ou de rede	467
Verifique se outros volumes no grupo de política de QoS têm atividade excepcionalmente alta	467
Mover interfaces lógicas (LIFs)	468
Execute operações de eficiência de armazenamento em horários de menor movimento	468
Adicionar discos e realocar dados	469
Como habilitar o Flash Cache em um nó pode melhorar o desempenho da carga de trabalho	470
Como habilitar o Flash Pool em um agregado de armazenamento pode melhorar o desempenho da carga de trabalho	470
Verificação de integridade da configuração do MetroCluster	471
Verificação da configuração do MetroCluster	471
Mover cargas de trabalho para um agregado diferente	472
Mover cargas de trabalho para um nó diferente	473
Mover cargas de trabalho para um agregado em um nó diferente	474
Mover cargas de trabalho para um nó em um par de HA diferente	476
Mover cargas de trabalho para outro nó em um par de HA diferente	478
Use as configurações de política de QoS para priorizar o trabalho neste nó	479
Remover volumes e LUNs inativos	480
Adicionar discos e executar reconstrução de layout agregado	480
Configurar uma conexão entre um servidor do Unified Manager e um provedor de dados externo	481
Dados de desempenho que podem ser enviados para um servidor externo	481
Configurar o Graphite para receber dados de desempenho do Unified Manager	482

Configurar uma conexão de um servidor do Unified Manager para um provedor de dados externo . . .	483
Monitorar e gerenciar a integridade do cluster	486
Introdução ao monitoramento de integridade do Active IQ Unified Manager	486
Capacidade física e lógica	486
Unidades de medida de capacidade	486
Recursos de monitoramento de integridade do Unified Manager	487
Interfaces do Unified Manager usadas para gerenciar a integridade do sistema de armazenamento . .	488
Gerenciando e monitorando clusters e integridade de objetos de cluster	489
Entenda o monitoramento de cluster	489
Veja a lista de clusters e detalhes	491
Verifique a integridade dos clusters em uma configuração MetroCluster	491
Visualizar o status de integridade e capacidade de todos os clusters do SAN Array	493
Ver a lista de nós e detalhes	494
Gerar um relatório de inventário de hardware para renovação de contrato	495
Veja a lista e os detalhes da VM de armazenamento	495
Veja a lista agregada e os detalhes	496
Ver informações sobre a capacidade do FabricPool	496
Ver detalhes do pool de armazenamento	498
Veja a lista de volumes e detalhes	498
Ver detalhes sobre ações NFS	499
Ver detalhes sobre ações SMB/CIFS	500
Veja a lista de cópias do Snapshot	501
Excluir cópias do Snapshot	501
Calcular espaço recuperável para cópias de Snapshot	502
Descrição das janelas e caixas de diálogo de objetos de cluster	503
Fluxos de trabalho e tarefas comuns de saúde do Unified Manager	503
Monitorar e solucionar problemas de disponibilidade de dados	504
Resolver problemas de capacidade	511
Gerenciar limites de saúde	513
Gerenciar objetivos de segurança do cluster	518
Gerenciar operações de backup e restauração	530
Gerenciar scripts	546
Gerenciar e monitorar grupos	549
Priorizar eventos de objetos de armazenamento usando anotações	557
Envie um pacote de suporte por meio da interface da web e do console de manutenção	566
Tarefas e informações relacionadas a vários fluxos de trabalho	573
Proteger e restaurar dados	632
Criar, monitorar e solucionar problemas de relacionamentos de proteção	632
Tipos de proteção SnapMirror	632
Configurar relacionamentos de proteção no Unified Manager	634
Executar failover e failback de relacionamento de proteção	636
Resolver uma falha de trabalho de proteção	640
Resolver problemas de atraso	643
Gerenciar e monitorar relacionamentos de proteção	645
Exibir status de proteção de volume	645

Exibir relacionamentos de proteção de volume	647
Monitorar LUNs em um relacionamento de grupo de consistência	648
Crie um relacionamento de proteção SnapVault na visualização Saúde: Todos os volumes	649
Crie um relacionamento de proteção SnapVault na página de detalhes Volume/Saúde	650
Crie um relacionamento de proteção SnapMirror na visualização Saúde: Todos os volumes	651
Crie um relacionamento de proteção SnapMirror na página de detalhes Volume/Saúde	652
Crie um relacionamento SnapMirror com replicação flexível de versão	654
Crie relacionamentos SnapMirror com replicação flexível de versão com opção de backup	655
Configurar as definições de eficiência do destino	656
Crie agendamentos SnapMirror e SnapVault	656
Crie relacionamentos em cascata ou em fanout para estender a proteção de um relacionamento de proteção existente	657
Editar relacionamentos de proteção na página Relacionamentos de Volume	658
Editar relacionamentos de proteção na página de detalhes de Volume/Saúde	658
Crie uma política SnapMirror para maximizar a eficiência de transferência	659
Crie uma política do SnapVault para maximizar a eficiência da transferência	659
Abortar uma transferência ativa de proteção de dados na página Relacionamentos de Volume	660
Abortar uma transferência ativa de proteção de dados na página de detalhes de Volume/Saúde	661
Desative um relacionamento de proteção na página Relacionamentos de Volume	662
Desativar uma relação de proteção na página de detalhes de Volume/Saúde	663
Interromper um relacionamento SnapMirror na página Relacionamentos de Volume	663
Remover um relacionamento de proteção da página Relacionamentos de Volume	664
Retomar transferências agendadas em um relacionamento desativado na página Relacionamentos de Volume	664
Retomar transferências agendadas em um relacionamento desativado na página de detalhes de Volume/Saúde	665
Inicializar ou atualizar relacionamentos de proteção na página Relacionamentos de Volume	666
Inicializar ou atualizar relacionamentos de proteção na página de detalhes de Volume/Saúde	667
Ressincronizar relacionamentos de proteção na página Relacionamentos de Volume	668
Relações de proteção reversa na página Relações de Volume	669
Restaurar dados usando as páginas Volume e Detalhes do Volume/Saúde	670
O que são pools de recursos	671
Criar pools de recursos	671
Editar pools de recursos	672
Ver inventário de pools de recursos	672
Adicionar membros do pool de recursos	672
Remover agregados de pools de recursos	673
Excluir pools de recursos	673
Monitorar relacionamentos de proteção de recuperação de desastres de VM de armazenamento	674
Entenda as associações de VM de armazenamento	676
Requisitos de SVM e pool de recursos para oferecer suporte a serviços de armazenamento	678
Quais são os empregos	679
Monitorar trabalhos	679
Ver detalhes do trabalho	680
Abortar trabalhos	680

Repetir uma tarefa de proteção com falha	680
Descrição das janelas e caixas de diálogo de relacionamentos de proteção	681
Gerar relatórios personalizados	724
Relatórios do Unified Manager	724
Pontos de acesso para geração de relatórios	724
Entenda os relatórios	726
Entenda a relação de exibição e relatório	726
Tipos de relatórios	727
Limitações de relatórios	729
Trabalhar com relatórios	729
Fluxo de trabalho do relatório	729
Início rápido de relatórios	730
Pesquisar um relatório agendado	733
Personalizar relatórios	733
Baixar relatórios	737
Agendar relatórios	737
Agendar um relatório	737
Gerenciar agendamentos de relatórios	740
Relatórios personalizados de amostra	742
Personalizar relatórios de armazenamento em cluster	743
Personalizar relatórios de capacidade agregada	746
Personalizar relatórios de capacidade de volume	748
Personalize relatórios de capacidade do Qtree	751
Personalizar relatórios de compartilhamento NFS	752
Personalizar relatórios de VM de armazenamento	754
Personalizar relatórios de relacionamento de volume	755
Personalizar relatórios de desempenho de volume	759
Relatórios de exemplo do Microsoft Excel	760
Crie um relatório para mostrar uma tabela e um gráfico de capacidade agregada	760
Crie um relatório para mostrar gráficos de capacidade total agregada versus capacidade disponível	763
Crie um relatório para visualizar gráficos de capacidade de volume disponíveis	766
Crie um relatório para visualizar agregados que tenham mais IOPS disponíveis	768
Gerenciar armazenamento usando APIs REST	771
Comece a usar as APIs Active IQ Unified Manager	771
Público para este conteúdo	771
Acesso e categorias da API do Active IQ Unified Manager	771
Serviços REST oferecidos no Active IQ Unified Manager	773
Versão da API no Active IQ Unified Manager	774
Recursos de armazenamento no ONTAP	774
Acesso e autenticação da API REST no Active IQ Unified Manager	775
Autenticação	777
Códigos de status HTTP usados no Active IQ Unified Manager	778
Recomendações para usar as APIs do Active IQ Unified Manager	779
Registros para solução de problemas	779
Objetos de trabalho processos assíncronos	780

Olá servidor API	781
APIs REST do Unified Manager	785
Gerenciar objetos de armazenamento em um data center usando APIs	786
Acesse APIs ONTAP por meio de acesso proxy	792
Executar tarefas administrativas usando APIs	794
Gerenciar usuários usando APIs	796
Visualizar métricas de desempenho usando APIs	797
Ver trabalhos e detalhes do sistema	808
Gerencie eventos e alertas usando APIs	809
Gerencie cargas de trabalho usando APIs	812
Fluxos de trabalho de API comuns para gerenciamento de armazenamento	821
Entenda as chamadas de API usadas nos fluxos de trabalho	821
Determinar problemas de espaço em agregados usando APIs	822
Determinar problemas em objetos de armazenamento usando APIs de eventos	824
Solucionar problemas de volumes ONTAP usando APIs de gateway	825
Fluxos de trabalho de API para gerenciamento de carga de trabalho	829
Avisos legais	856
Direitos autorais	856
Marcas Registradas	856
Patentes	856
Política de Privacidade	856
Código aberto	856

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

Começar

Instruções de início rápido para instalações do VMware

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

Requisitos do sistema

- Sistema operacional: VMware ESXi 8.0
- RAM: 12 GB
- CPU: 9572 MHz no total
- Espaço livre em disco: 5 GB (provisionamento fino), 152 GB (provisionamento espesso)

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

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 de rede que seja acessível ao seu vSphere Client.
3. No diretório onde você baixou o `.tar` arquivo, digite o `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz` comando. + O necessário OVA arquivo, um certificado raiz e um README arquivo são descompactados no diretório de destino.

Verificar integridade

Você pode verificar a integridade do OVA arquivo seguindo os passos fornecidos no README arquivo.

Instalar o Unified Manager

1. No vSphere Client, clique em **Arquivo > Implantar modelo OVF**.
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 arquivo. 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 configuração estática, insira as informações necessárias em todos os campos. Não é necessário adicionar informações para o campo **DNS secundário**.
 - 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 aba Console para visualizar o processo de inicialização.
7. Configurar o fuso horário.
8. Insira um nome de usuário e uma senha de manutenção do Unified Manager.

No final da instalação, as informações para se conectar à interface 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 Red Hat Enterprise Linux física ou virtual.

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 no total
- Espaço livre em disco: 100 GB de espaço em disco no /opt/netapp/data diretório, 50 GB na partição raiz. Para montagem separada /opt e /var/log diretórios, certifique-se de que /opt tem 15 GB, /var/log tem 16 GB e /tmp tem 10 GB de espaço livre.

Para obter requisitos detalhados do sistema e informações sobre como instalar o produto em um local seguro, consulte o ["Requisitos para instalar o Unified Manager"](#) e o ["Matriz de Interoperabilidade"](#).

Instalar o Active IQ Unified Manager

Baixe o instalador

1. Baixe o ActiveIQUnifiedManager-<version>.zip pacote de instalação junto com certificado de assinatura de código(.pem) e assinatura digital(.sig).
2. No diretório onde você baixou o arquivo de instalação, execute:

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

Verificar integridade

Execute os seguintes comandos para verificar a integridade do pacote do instalador:

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

Verificar configuração do repositório

Os procedimentos para configurar um repositório do 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 do Red Hat Enterprise Linux.

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

Instalar o Unified Manager

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

Para instalar o Unified Manager, execute o seguinte comando, como usuário `root` ou usando `sudo` , do diretório onde 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 conectar-se à interface web do Unified Manager são exibidas. Se você não conseguir se conectar à interface da web, consulte o `README` arquivo fornecido 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 de armazenamento de dados, disponibilidade, desempenho e proteção.

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: 9572 MHz no total

- 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 requisitos detalhados do sistema, consulte o ["Requisitos para instalar o Unified Manager"](#) e ["Matriz de Interoperabilidade"](#).

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.

Instalar o Unified Manager

Para instalar o Unified Manager, certifique-se de ter o Microsoft .NET 4.5.2 ou uma versão posterior instalado. 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. Efetue login no Windows usando a conta de administrador local padrão.
2. No diretório onde você baixou o arquivo de instalação, clique com o botão direito do mouse e execute o arquivo executável (.exe) do Unified Manager 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 de conexão de banco de dados, insira a senha root do MySQL.
5. Siga as instruções restantes para concluir a instalação.
6. Clique em **Concluir** no final da instalação e a interface de usuário da Web do Unified Manager será exibida.

Instalar o Unified Manager em sistemas VMware vSphere

Introdução ao Active IQ Unified Manager

O Active IQ Unified Manager (antigo OnCommand Unified Manager) permite que você monitore e gerencie a integridade e o desempenho dos seus sistemas de armazenamento ONTAP a partir de 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, a disponibilidade, a proteção e o status de desempenho dos sistemas de armazenamento monitorados.

Informações relacionadas

["Ferramenta de Matriz de Interoperabilidade da NetApp"](#)

O que o servidor Unified Manager faz

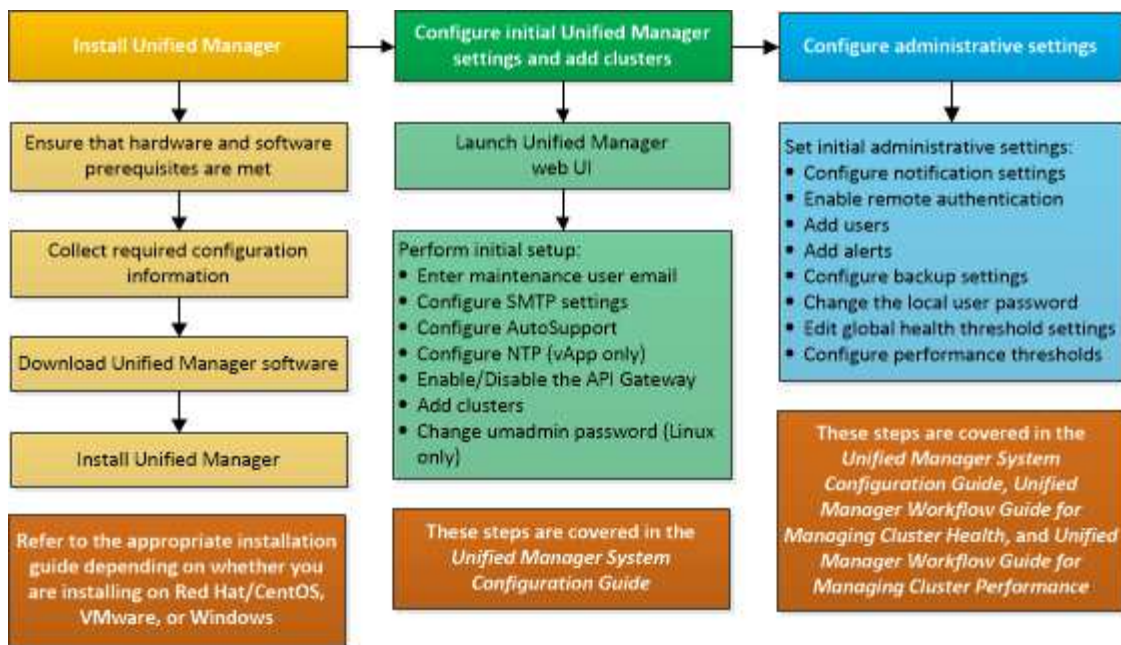
A infraestrutura do servidor do Unified Manager consiste em uma unidade de coleta de dados, um banco de dados e um servidor de aplicativos. Ele fornece serviços de infraestrutura, como descoberta, monitoramento, controle de acesso baseado em funções (RBAC), auditoria e registro.

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

Visão geral da sequência de instalação

O fluxo de trabalho de instalação descreve as tarefas que você deve executar antes de poder 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, certifique-se de que 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 Unified Manager. Se precisar aplicar quaisquer medidas de segurança ao servidor do Unified Manager, você deverá fazer 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 Conhecimento.

["Suportabilidade para medidas de segurança aplicadas ao Active IQ Unified Manager para Data ONTAP"](#)

Informações relacionadas

Para mais informações, consulte ["Ferramenta de Matriz de Interoperabilidade da 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 a níveis de desempenho aceitáveis.

Configuração de hardware	Configurações recomendadas
BATER	12 GB (requisito mínimo de 8 GB)
Processadores	4 CPUs

Configuração de hardware	Configurações recomendadas
Capacidade do ciclo da CPU	9572 MHz total (requisito mínimo 9572 MHz)
Espaço livre em disco	• 5 GB (provisionamento fino) • 152 GB (provisionamento denso)

O Unified Manager pode ser instalado em sistemas com pouca memória, mas os 12 GB de RAM recomendados garantem que haja memória suficiente disponível para um desempenho ideal e para que o sistema possa acomodar clusters e objetos de armazenamento adicionais conforme sua configuração cresce. Você não deve definir nenhum limite de memória na VM onde o Unified Manager está implantado e não deve habilitar nenhum recurso (por exemplo, balão) que impeça 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 você instalar uma segunda instância do Unified Manager. Para mais informações, consulte ["Guia de práticas recomendadas do Unified Manager"](#).

A troca de páginas de memória afeta negativamente o desempenho do sistema e do aplicativo de gerenciamento. Competir por recursos de CPU que não estão disponíveis devido à utilização geral do host pode prejudicar o desempenho.

Requisito de 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. Outros aplicativos podem consumir recursos do sistema e reduzir drasticamente o desempenho do Unified Manager.

Requisitos de espaço para backups

Se você planeja usar o recurso de backup e restauração do Unified Manager, aloque capacidade adicional para que o diretório ou disco “data” tenha 150 GB de espaço. Um backup pode ser gravado em um destino local ou 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 do host

O sistema físico ou virtual no qual você instala o Unified Manager deve ser configurado de forma que você possa ping o nome do host do próprio host. No caso de configuração IPv6, você deve verificar se ping6 para o nome do host for 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 interface da web do produto. Se você configurou um endereço IP estático para sua rede durante a implantação, você designou um nome para o host da rede. Se você configurou a rede usando DHCP, deverá obter o nome do host do DNS.

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

Requisitos de instalação e software VMware

O sistema VMware vSphere no qual você instala o Unified Manager requer uma versão

específica do sistema operacional e versões específicas do software de suporte.

Software do sistema operacional

O sistema operacional suportado é o VMware ESXi 8.0.



O Unified Manager OVA em sistemas VMware vSphere executa o Debian OS 12 (bookworm) internamente. Para obter informações sobre as versões do hardware da máquina virtual que as versões suportadas dos servidores ESXi podem suportar, consulte a documentação do 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 atualizada de versões suportadas do ESXi.

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

O horário do servidor VMware ESXi deve ser o mesmo que o horário do servidor NTP para que o dispositivo virtual funcione corretamente. Sincronizar o horário do servidor VMware ESXi com o horário do servidor NTP evita falhas de horário.

Requisitos de instalação

O VMware High Availability para o appliance virtual Unified Manager é suportado.

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

Se a implantação falhar usando seu ambiente habilitado para Alta Disponibilidade devido a recursos insuficientes, talvez seja necessário modificar as Opções da Máquina Virtual dos Recursos do Cluster desabilitando a Prioridade de Reinicialização da VM e deixando a Resposta de Isolamento do Host ativada.



Ao instalar ou atualizar o Unified Manager, o software de terceiros e os patches de segurança 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 autônoma de nenhum componente de terceiros.

Navegadores suportados

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

A Matriz de Interoperabilidade tem a lista de versões de navegadores suportadas.

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

Para todos os navegadores, desabilitar os bloqueadores de 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, verifique também a lista de navegadores suportados pelo IdP.

Requisitos de protocolo e porta

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

Conexões com o servidor do Unified Manager

Em instalações típicas, você não precisa especificar números de porta ao se conectar à interface de usuário 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 inserir `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
Interface da Web do Unified Manager	HTTP	80	Usado para acessar a interface da web do Unified Manager; redireciona automaticamente para a porta segura 443.
Interface da Web do Unified Manager e programas que usam APIs	HTTPS	443	Usado para acessar com segurança a interface da Web do Unified Manager ou para fazer chamadas de API; chamadas de API só podem ser feitas usando HTTPS.
Console de manutenção	SSH/SFTP	22	Usado para acessar o console de manutenção e recuperar pacotes de suporte.
Linha de comando do Linux	SSH/SFTP	22	Usado para acessar a linha de comando do Red Hat Enterprise Linux e recuperar pacotes de suporte.
Log de sistema	UDP	514	Usado para acessar mensagens EMS baseadas em assinatura de sistemas ONTAP e para criar eventos com base nas mensagens.

Interface	Protocolo	Porta	Descrição
DESCANSAR	HTTPS	9443	Usado para acessar eventos EMS baseados em API REST em tempo real de sistemas ONTAP autenticados.
Banco de dados MySQL	MySQL	3306	Usado para habilitar o acesso do OnCommand Workflow Automation e do OnCommand API Services ao Unified Manager.
Corretor AMQP QPID	TCP/IP	56072	Usado para comunicação de mensagens internas.
Corretor AMQP QPID	WebSocket sobre TCP	56080	Usado para escutar nesta porta mensagens recebidas do ONTAP (agente de nuvem).
Corretor AMQP QPID	WebSocket sobre TCP	56443	Usado para escutar nesta porta mensagens recebidas do ONTAP (agente de nuvem). A comunicação por esta porta suporta criptografia fornecida por TLS ou SSL.



A porta padrão do MySQL, 3306, é restrita apenas ao host local 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 para outros hosts usando o Control access to MySQL port 3306 opção no console de manutenção. Para obter informações, consulte ["Opções adicionais de menu"](#). As portas usadas para comunicação HTTP e HTTPS (portas 80 e 443) podem ser alteradas usando o console de manutenção do Unified Manager. Para mais informações, consulte ["Menus do console de manutenção"](#).

Conexões do servidor do Unified Manager

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

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

O servidor do Unified Manager se conecta usando os seguintes protocolos e portas aos sistemas de

armazenamento gerenciados, servidores e outros componentes:

Destino	Protocolo	Porta	Descrição
Sistema de armazenamento	HTTPS	443/TCP	Usado para monitorar e gerenciar sistemas de armazenamento.  Se você estiver usando esta porta ou qualquer outra porta para se conectar ao VMware vCenter Server ou ao servidor ESXi, certifique-se de que a porta esteja disponível e possa ser conectada em um site seguro.
Sistema de armazenamento	NDMP	10000/TCP	Usado para determinadas operações de restauração de Snapshot.
Servidor AutoSupport	HTTPS	443	Usado para enviar informações do AutoSupport . É necessário 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 e-mail

Destino	Protocolo	Porta	Descrição
SMTP	25	Usado para enviar e-mails de notificação de alerta.	Remetente de armadilha SNMP
SNMPv1 ou SNMPv3	162/UDP	Usado para enviar notificações de alerta de traps SNMP.	Servidor 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 o horário no servidor do Unified Manager com um servidor de horário NTP externo. (Somente sistemas VMware)	Log de sistema

Complete a planilha

Antes de instalar e configurar o Unified Manager, você deve ter informações específicas sobre seu ambiente prontamente disponíveis. Você pode registrar as informações na planilha.

Informações de instalação do Unified Manager

Os detalhes necessários para instalar o Unified Manager.

Sistema no qual o software é implantado	Seu valor
Endereço IP do servidor ESXi	
Hospedar nome de domínio totalmente qualificado	
Endereço IP do host	
Máscara de rede	
Endereço IP do gateway	
Endereço DNS primário	
Endereço DNS secundário	
Domínios de pesquisa	

Sistema no qual o software é implantado	Seu valor
Nome de usuário de manutenção	
Senha do usuário de manutenção	

Informações de configuração do Unified Manager

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

Contexto	Seu valor
Endereço de e-mail do usuário de manutenção	
Servidor NTP	
Nome do host ou endereço IP do servidor SMTP	
Nome de usuário SMTP	
Senha SMTP	
Porta SMTP	25 (Valor padrão)
E-mail de onde as notificações de alerta são enviadas	
Nome do host ou endereço IP do servidor de autenticação	
Nome do administrador do Active Directory ou nome distinto do vínculo LDAP	
Senha do Active Directory ou senha de vinculação LDAP	
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 da armadilha SNMP	
Porta SNMP	

Informações do cluster

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

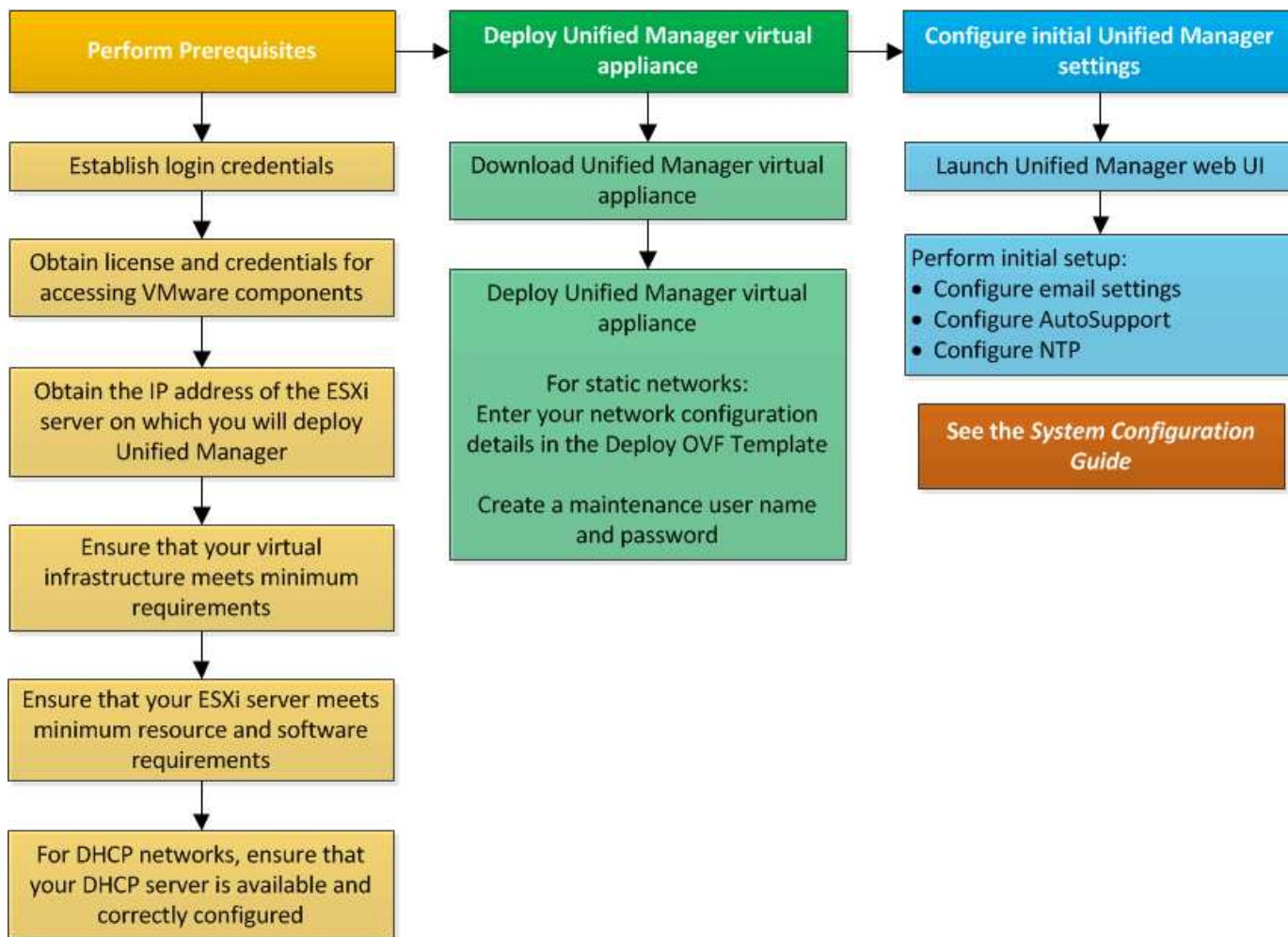
Cluster 1 de N	Seu valor
Nome do host ou endereço IP de gerenciamento de cluster	
 O administrador deve ter recebido a função “admin”. Nome de usuário do administrador ONTAP	
Senha do administrador do ONTAP	
Protocolo	HTTPS

Instalar, atualizar e remover o software Unified Manager

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

Visão geral do processo de implantação

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



Implantar o Unified Manager

A implantação do Unified Manager inclui o download do 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 do usuário da Web.

Antes de começar

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

Ver "[Requisitos do sistema](#)".

- Certifique-se de ter 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 appliance virtual do Unified Manager
 - Detalhes sobre o data center, como espaço de armazenamento no datastore e requisitos de memória
 - O IPv6 deve ser habilitado no host se você planeja usar o 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 pelo 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.

Após concluir a implantação e a configuração inicial, você pode adicionar clusters ou configurar configurações de rede adicionais no console de manutenção e, em seguida, acessar a interface da web.

Passos

1. Siga os passos em "[Baixar o Unified Manager](#)".
2. Além disso, siga os passos em "[Implantar o appliance virtual do Unified Manager](#)".

Baixe o arquivo de instalação do Unified Manager

Baixe o 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 contendo o software Unified Manager configurado para um dispositivo virtual.

Passos

1. Efetue login no site de suporte da NetApp e navegue até a página de download do Unified Manager:

"[Site de suporte da NetApp](#)"
2. Selecione a versão necessária do Unified Manager e aceite o contrato de licença de usuário final (EULA).
3. Baixe e salve o `.tar` arquivo para instalação do VMware vSphere em um diretório local ou diretório de rede que seja acessível ao seu vSphere Client.
4. Verifique a soma de verificação para garantir que o software foi baixado corretamente.
5. Navegue até o diretório onde 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 necessário OVA arquivo, um certificado raiz e um README arquivo para o Unified Manager são descompactados no diretório de destino.

6. Verifique a integridade do OVA arquivo seguindo os passos fornecidos no README arquivo.

Implantar o appliance virtual do Unified Manager

Após baixar o arquivo de instalação, implante o Unified Manager como um dispositivo virtual. Use o vSphere Web Client para implantar o dispositivo virtual em um servidor ESXi. Quando você implanta o dispositivo virtual, uma máquina virtual é criada.

Antes de começar

Você deve revisar os requisitos do sistema. Faça as alterações necessárias antes de implantar o appliance virtual do Unified Manager.

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

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

Se você usar o Protocolo de Configuração Dinâmica de Hosts (DHCP), verifique se o servidor DHCP está disponível e se as configurações do adaptador de rede DHCP e da máquina virtual (VM) estão corretas. O DHCP é configurado por padrão.

Se você usar uma configuração de rede estática, certifique-se de que o endereço IP não esteja duplicado na mesma sub-rede e que as entradas apropriadas do servidor DNS tenham sido 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 appliance virtual do Unified Manager
- Detalhes sobre o data center, como disponibilidade de espaço de armazenamento
- Se você não estiver usando DHCP, obtenha os endereços IPv4 ou IPv6 para os dispositivos de rede aos quais você planeja se conectar:
 - Nome de domínio totalmente qualificado (FQDN) do host
 - Endereço IP do host
 - Máscara de rede
 - Endereço IP do gateway padrão
 - Endereços DNS primários e secundários
 - Domínios de pesquisa

A partir do Unified Manager 9.8, o VMware Tools foi substituído pelo 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 interface da Web do Unified Manager, você poderá ver um aviso do navegador sobre certificados não confiáveis.

O VMware High Availability para o appliance virtual Unified Manager é suportado.

Passos

1. No vSphere Client, clique em **Arquivo > Implantar modelo OVF**.
2. Conclua o assistente Implantar modelo OVF para implantar o appliance virtual do Unified Manager.

Na página Detalhes da revisão:

- Verifique os detalhes da seção Editora. A mensagem **Entrust Code Signing - OVCS2 (Trusted certificate)** confirma a integridade do arquivo baixado OVA arquivo. + Se você vir a mensagem **Entrust Code Signing - OVCS2 (Certificado inválido)**, 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 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 seja exclusivo para o host no qual está implantado, que ainda não esteja em uso e que tenha uma entrada DNS válida.
3. Depois que o appliance virtual do Unified Manager for implantado no servidor ESXi, ligue a VM clicando com o botão direito do mouse nela e selecionando **Ligar**.



Se a operação de inicialização falhar devido a recursos insuficientes, adicione recursos e tente instalar novamente.

4. Clique na aba **Console**.

O processo de inicialização 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 do 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 seus dispositivos gerenciados. Se seus sistemas de armazenamento e o servidor de gerenciamento estiverem configurados com o mesmo servidor NTP, eles se referirão ao mesmo instante no tempo, mesmo que pareçam diferentes. Por exemplo, se você criar uma cópia do Snapshot usando um dispositivo configurado com um fuso horário diferente daquele do servidor de gerenciamento, o registro de data e hora será o horário do servidor de gerenciamento.

6. Se nenhum serviço DHCP estiver disponível ou se houver um erro nos detalhes da configuração de rede estática, selecione uma das seguintes opções:

Se você usar...	Então faça isto...
DHCP	Selecione Repetir DHCP. Se você planeja usar DHCP, certifique-se de que ele esteja configurado corretamente. Se você usar uma rede habilitada para DHCP, as entradas do servidor FQDN e DNS serão fornecidas ao dispositivo virtual automaticamente. Se o DHCP não estiver configurado corretamente com o DNS, o nome do host “UnifiedManager” será automaticamente atribuído e associado ao certificado de segurança. Se você não configurou uma rede habilitada para DHCP, deverá inserir manualmente as informações de configuração de rede.

Se você usar...	Então faça isto...
Uma configuração de rede estática	a. Selecione Insira os detalhes para configuração de rede estática. O processo de configuração leva alguns minutos para ser concluído. b. Confirme os valores inseridos e selecione S.

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 az, seguida por qualquer combinação de -, az ou 0-9.

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

O console da VM exibe a URL da interface do usuário da Web do Unified Manager.

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

Atualizar o Unified Manager

Você pode atualizar o Active IQ Unified Manager para a versão 9.16 somente a partir da versão 9.13 ou 9.14.

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

Se o Unified Manager estiver pareado com uma instância do OnCommand Workflow Automation e houver novas versões de software disponíveis para ambos os produtos, você deverá desconectar os dois produtos e configurar uma nova conexão do Workflow Automation após executar as atualizações. Se você estiver realizando uma atualização para apenas um dos produtos, faça login no Workflow Automation após a atualização e verifique se ele ainda está adquirindo dados do Unified Manager.

Passos

1. Siga os passos em ["Baixe a imagem ISO do Unified Manager"](#).
2. Além disso, siga os passos descritos em ["Atualizar o Unified Manager"](#).

Caminho de atualização com suporte para versões do Unified Manager

O Active IQ Unified Manager oferece suporte a um caminho de atualização específico para cada versão.

Nem todas as versões do Unified Manager podem executar uma atualização local para versões posteriores. As atualizações do Unified Manager são limitadas a um modelo N-2, o que significa que uma atualização só pode ser realizada nas próximas 2 versões em todas as plataformas. Por exemplo, você pode executar uma atualização do Unified Manager 9.16 somente a partir 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 para uma das versões suportadas primeiro e depois atualizada para a versão atual.

Por exemplo, se a sua versão instalada for o Unified Manager 9.9 e você quiser atualizar para o Unified Manager 9.14, siga uma sequência de atualizações.

Caminho de atualização de exemplo:

1. Atualização 9.11 → 9.13
2. Atualização 9.13 → 9.14
3. Atualização 9.13 → 9.16
4. Atualização 9.14 → 9.16

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

Baixe o arquivo de atualização do Unified Manager

Antes de atualizar o Unified Manager, baixe o 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. Efetue login no site de suporte da NetApp :

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

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

Atualizar o appliance virtual do Unified Manager

Você pode atualizar o appliance virtual Active IQ Unified Manager das versões 9.13 ou 9.14 para 9.16.

Antes de começar

Garanta o seguinte:

- 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.

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

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

- Para usuários do vSphere 6.5 e 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 retenção de dados de desempenho por 13 meses ou alterá-las para 6 meses. Após a confirmação, os dados de desempenho histórico são eliminados 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 estará disponível. Você deve concluir todas as operações em execução antes de atualizar o Unified Manager.

Se você tiver pareado o Workflow Automation e o Unified Manager, deverá atualizar manualmente o nome do host no Workflow Automation.

Passos

1. No vSphere Client, clique em **Início > Inventário > 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 **Resumo > Comandos > Desligar convidado**.
4. Crie uma cópia de backup, como um snapshot ou um clone, da VM do Unified Manager para criar um backup consistente com o aplicativo.
5. No vSphere Client, ligue a VM do Unified Manager.
6. Inicie o VMware Remote Console.
7. Clique no ícone **CDROM** e selecione **Conectar ao arquivo de imagem de disco (.iso)**.
8. Selecione o `ActiveIQUnifiedManager-<version>-virtual-update.iso` arquivo e clique em **Abrir**.
9. Clique na aba **Console**.
10. Efetue login no console de manutenção do Unified Manager.
11. No Menu Principal, selecione **Atualizar**.

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

12. Tipo `y` para continuar.

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

13. Tipo `y` para continuar.

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

14. Pressione qualquer tecla para continuar.

Você será desconectado automaticamente do console de manutenção.

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

Você pode iniciar a interface da Web em uma nova janela em um navegador da Web compatível e efetuar login para usar a versão atualizada do Unified Manager. Observe que você precisa aguardar a conclusão do processo de descoberta antes de executar qualquer tarefa na interface do usuário.

Reinicie a máquina virtual do Unified Manager

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

Antes de começar

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

Você também pode reiniciar a máquina virtual a partir do vSphere usando a opção VMware **Restart Guest**. Consulte ["o cmdlet Restart-VMGuest na referência do CMDLET VMware vSphere PowerCLI da Broadcom."](#)

Passos

1. No console de manutenção, selecione **Configuração do sistema > Reinicializar máquina virtual**.
2. Inicie a interface de usuário da Web do Unified Manager no seu navegador e faça login.

Remover o 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 Unified Manager com um servidor de automação de fluxo de trabalho 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 **Início > Inventário > VMs e Modelos**.
3. Selecione a VM que você deseja remover e clique na aba **Resumo**.
4. Se a VM estiver em execução, clique em **Energia > Desligar convidado**.
5. Clique com o botão direito do mouse na VM que você deseja remover e clique em **Excluir do disco**.

Instalar o Unified Manager em sistemas Linux

Introdução ao Active IQ Unified Manager

O Active IQ Unified Manager (antigo OnCommand Unified Manager) permite que você monitore e gerencie a integridade e o desempenho dos seus sistemas de armazenamento ONTAP a partir de 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, a disponibilidade, a proteção e o status de desempenho dos sistemas de armazenamento monitorados.

Informações relacionadas

["Ferramenta de Matriz de Interoperabilidade da NetApp"](#)

O que o servidor Unified Manager faz

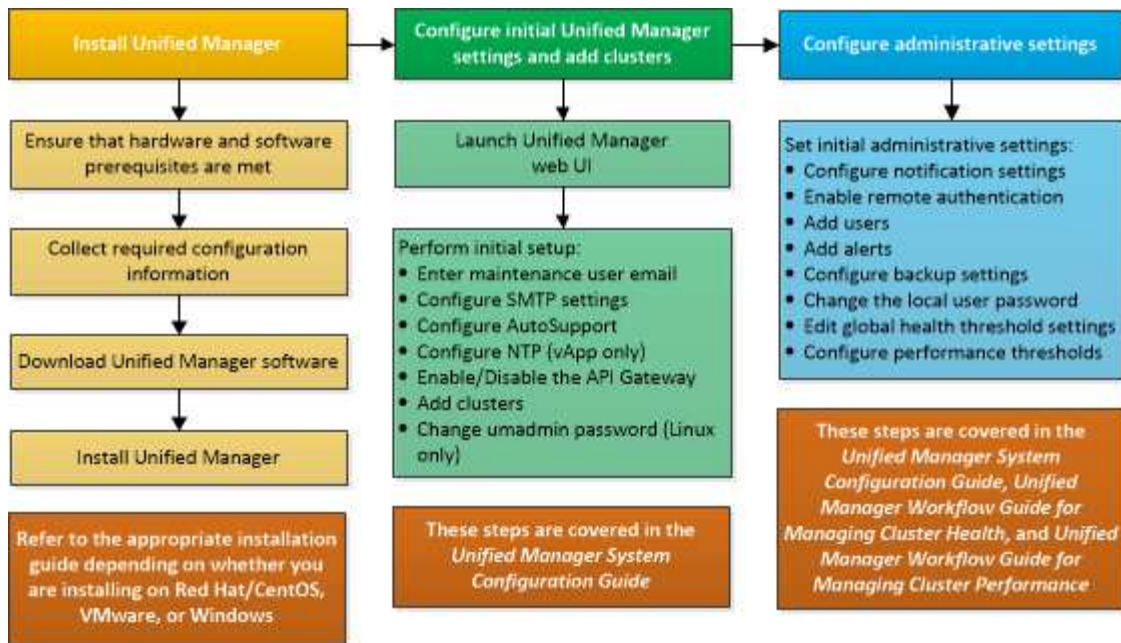
A infraestrutura do servidor do Unified Manager consiste em uma unidade de coleta de dados, um banco de dados e um servidor de aplicativos. Ele fornece serviços de infraestrutura, como descoberta, monitoramento, controle de acesso baseado em funções (RBAC), auditoria e registro.

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

Visão geral da sequência de instalação

O fluxo de trabalho de instalação descreve as tarefas que você deve executar antes de poder 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, certifique-se de que 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 Unified Manager. Se precisar aplicar quaisquer medidas de segurança ao servidor do Unified Manager, você deverá fazer 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 Conhecimento.

["Suportabilidade para medidas de segurança aplicadas ao Active IQ Unified Manager para Data ONTAP"](#)

Informações relacionadas

["Ferramenta de Matriz de Interoperabilidade da 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 a níveis de desempenho aceitáveis.

Configuração de hardware	Configurações recomendadas
BATER	12 GB (requisito mínimo de 8 GB)
Processadores	4 CPUs

Configuração de hardware	Configurações recomendadas
Capacidade do ciclo da CPU	9572 MHz total (requisito mínimo 9572 MHz)
Espaço livre em disco	150 GB, onde a capacidade é alocada da seguinte forma: • 50 GB alocados para a partição raiz • 100 GB de espaço livre em disco alocado para o <code>/opt/netapp/data</code> diretório, que é montado em uma unidade LVM ou em um disco local separado conectado ao sistema de destino  Para montagem separada <code>/opt</code> e <code>/var/log</code> diretórios, 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> O diretório deve ter pelo menos 10 GB de espaço livre.

O Unified Manager pode ser instalado em sistemas com pouca memória, mas os 12 GB de RAM recomendados garantem que haja memória suficiente disponível para um desempenho ideal e para que o sistema possa acomodar clusters e objetos de armazenamento adicionais conforme sua configuração cresce. Você não deve definir nenhum limite de memória na VM onde o Unified Manager está implantado e não deve habilitar nenhum recurso (por exemplo, balão) que impeça 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 você instalar uma segunda instância do Unified Manager. Para mais informações, consulte o *Guia de Melhores Práticas*.

["Relatório Técnico 4621: Guia de Melhores Práticas do Unified Manager"](#)

A troca de páginas de memória afeta negativamente o desempenho do sistema e do aplicativo de gerenciamento. Competir por recursos de CPU que não estão disponíveis devido à utilização geral do host pode prejudicar o desempenho.

Requisito de 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. Outros aplicativos podem consumir recursos do sistema e reduzir drasticamente o desempenho do Unified Manager.

Requisitos de espaço para backups

Se você planeja usar o recurso de backup e restauração do Unified Manager, alocue capacidade adicional para que o diretório ou disco “data” tenha 150 GB de espaço. Um backup pode ser gravado em um destino local ou 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 do host

O sistema físico ou virtual no qual você instala o Unified Manager deve ser configurado de forma que você possa ping o nome do host do próprio host. No caso de configuração IPv6, você deve verificar se ping6 para o nome do host for 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 interface da web do produto. Se você configurou um endereço IP estático para sua rede durante a implantação, você designou um nome para o host da rede. Se você configurou a rede usando DHCP, deverá obter o nome do host do DNS.

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

Requisitos de instalação e software Linux

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

Software do sistema operacional

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

- Red Hat Enterprise Linux versões 8.x e 9.4, baseadas na arquitetura x86_64.

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

["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 um scanner de vulnerabilidades como o Qualys esteja instalado no seu sistema Linux devido a regulamentações da empresa. Você deve desabilitar o scanner de vulnerabilidades antes de instalar o Unified Manager para evitar que a instalação falhe.



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

Software de terceiros

O Unified Manager é implantado em um servidor web WildFly. O WildFly 26.1.3 é fornecido 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 conforme mencionado nas seções a seguir.

- MySQL Community Edition versão 8.4.4 (do repositório MySQL)
- OpenJDK versão 11.0.25 (do repositório do 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 (do repositório Red Hat Extra Packages for Enterprise Linux)



Você deve desligar uma instância em execução do Unified Manager antes de atualizar qualquer software de terceiros. Após a conclusão da instalação do software de terceiros, você pode reiniciar o Unified Manager.

Requisitos de autorização do usuário

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

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

Requisitos de instalação

As melhores práticas para instalar o Red Hat Enterprise Linux e os repositórios associados no seu sistema estão listadas abaixo. Sistemas instalados ou configurados de forma diferente, ou implantados externamente (na nuvem), podem exigir etapas adicionais, e o Unified Manager pode não ser executado corretamente nessas implantações.

- Você deve instalar o Red Hat Enterprise Linux de acordo com as práticas recomendadas do Red Hat e selecionar as seguintes opções padrão, o que requer a seleção do ambiente base “Servidor com GUI”.
- Ao instalar o Unified Manager no Red Hat Enterprise Linux, o sistema deve ter acesso ao repositório apropriado para que o programa de instalação possa acessar e instalar todas as dependências de software necessárias.
- Para o `yum` instalador para encontrar software dependente nos repositórios do 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 do Red Hat para obter informações sobre o Red Hat Subscription Manager.

- Você deve habilitar o repositório Extra Packages for Enterprise Linux (EPEL) para instalar com sucesso os utilitários de terceiros necessários no seu sistema.

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

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

- Se a versão correta do MySQL não estiver instalada, você deverá habilitar o repositório MySQL para instalar com sucesso o software MySQL no seu sistema.

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

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

- Você deve instalar apenas uma versão do Java no seu host do Unified Manager; caso contrário, o sistema pode não conseguir determinar qual versão usar. Ver "[Após atualizar o Java no host do Active IQ Unified Manager, os serviços não serão iniciados](#)".

Se o seu sistema não tiver acesso à Internet e os repositórios não forem espelhados de um sistema conectado à Internet para o sistema desconectado, você deverá seguir as instruções de instalação para determinar as dependências de software externo do seu sistema. Em seguida, você pode baixar o software necessário para o sistema conectado à Internet e copiá-lo. `.rpm` arquivos para o sistema no qual você planeja instalar o Unified Manager. Para baixar os artefatos 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 diferentes dos listados aqui. O software instalado dos repositórios do Red Hat foi projetado explicitamente para o Red Hat Enterprise Linux e está em conformidade com as práticas recomendadas do Red Hat (layouts de diretório, permissões e assim por diante). Softwares de outros locais podem não seguir essas diretrizes, o que pode causar falha na instalação do Unified Manager ou problemas com atualizações futuras.

Requisito da porta 443

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 interface da Web do administrador após instalar o Unified Manager. Executar o comando a seguir permite 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 "Servidor com GUI". Ele fornece os comandos usados pelas instruções de instalação do Unified Manager. Outros ambientes base podem exigir que você instale comandos adicionais para validar ou concluir a instalação. Se o `firewall-cmd` não estiver disponível em seu sistema, você deve instalá-lo executando o seguinte comando:

```
# sudo yum install firewalld
```

Entre em contato com seu departamento de TI antes de executar os comandos para verificar se suas políticas de segurança exigem um procedimento diferente.



THP (Transparent Huge Pages) deve ser desabilitado em sistemas Red Hat. Quando ativado, em alguns casos, pode fazer com que o Unified Manager seja desligado quando certos processos consomem muita memória e são encerrados.

Navegadores suportados

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

A Matriz de Interoperabilidade tem a lista de versões de navegadores suportadas.

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

Para todos os navegadores, desabilitar os bloqueadores de 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, verifique também a lista de navegadores suportados pelo IdP.

Requisitos de protocolo e porta

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

Conexões com o servidor do Unified Manager

Em instalações típicas, você não precisa especificar números de porta ao se conectar à interface de usuário 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 inserir `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
Interface da Web do Unified Manager	HTTP	80	Usado para acessar a interface da web do Unified Manager; redireciona automaticamente para a porta segura 443.
Interface da Web do Unified Manager e programas que usam APIs	HTTPS	443	Usado para acessar com segurança a interface da Web do Unified Manager ou para fazer chamadas de API; chamadas de API só podem ser feitas usando HTTPS.
Console de manutenção	SSH/SFTP	22	Usado para acessar o console de manutenção e recuperar pacotes de suporte.
Linha de comando do Linux	SSH/SFTP	22	Usado para acessar a linha de comando do Red Hat Enterprise Linux e recuperar pacotes de suporte.

Interface	Protocolo	Porta	Descrição
Banco de dados MySQL	MySQL	3306	Usado para habilitar o acesso do OnCommand Workflow Automation e do OnCommand API Services ao Unified Manager.
Log de sistema	UDP	514	Usado para acessar mensagens EMS baseadas em assinatura de sistemas ONTAP e para criar eventos com base nas mensagens.
DESCANSAR	HTTPS	9443	Usado para acessar eventos EMS baseados em API REST em tempo real de sistemas ONTAP autenticados.
Banco de dados MySQL	MySQL	3306	Usado para habilitar o acesso do OnCommand Workflow Automation e do OnCommand API Services ao Unified Manager.
Corretor AMQP QPID	TCP/IP	56072	Usado para comunicação de mensagens internas.
Corretor AMQP QPID	WebSocket sobre TCP	56080	Usado para escutar nesta porta mensagens recebidas do ONTAP (agente de nuvem).
Corretor AMQP QPID	WebSocket sobre TCP	56443	Usado para escutar nesta porta mensagens recebidas do ONTAP (agente de nuvem). A comunicação por esta porta suporta criptografia fornecida por TLS ou SSL.



A porta padrão do MySQL, 3306, é restrita apenas ao host local 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 para outros hosts usando o `Control access to MySQL port 3306` opção no console de manutenção. Para obter informações, consulte ["Opções adicionais de menu"](#). As portas usadas para comunicação HTTP e HTTPS (portas 80 e 443) podem ser alteradas usando o console de manutenção do Unified Manager. Para mais informações, consulte ["Menus do console de manutenção"](#).

Conexões do servidor do Unified Manager

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

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

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

Destino	Protocolo	Porta	Descrição
Sistema de armazenamento	HTTPS	443/TCP	Usado para monitorar e gerenciar sistemas de armazenamento.
Sistema de armazenamento	NDMP	10000/TCP	Usado para determinadas operações de restauração de Snapshot.
Servidor AutoSupport	HTTPS	443	Usado para enviar informações do AutoSupport. É necessário 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 e-mail
SMTP	25	Usado para enviar e-mails de notificação de alerta.	Remetente de armadilha SNMP

Destino	Protocolo	Porta	Descrição
SNMPv1 ou SNMPv3	162/UDP	Usado para enviar notificações de alerta de traps SNMP.	Servidor 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 o horário no servidor do Unified Manager com um servidor de horário NTP externo. (Somente sistemas VMware)	Log de sistema

Complete a planilha

Antes de instalar e configurar o Unified Manager, você deve ter informações específicas sobre seu ambiente prontamente disponíveis. Você pode registrar as informações na planilha.

Informações de instalação do Unified Manager

Os detalhes necessários para instalar o Unified Manager.

Sistema no qual o software é implantado	Seu valor
Hospedar nome de domínio totalmente qualificado	
Endereço IP do host	
Máscara de rede	
Endereço IP do gateway	
Endereço DNS primário	
Endereço DNS secundário	
Domínios de pesquisa	
Nome de usuário de manutenção	
Senha do usuário de manutenção	

Informações de configuração do Unified Manager

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

Contexto	Seu valor
Endereço de e-mail do usuário de manutenção	
Nome do host ou endereço IP do servidor SMTP	
Nome de usuário SMTP	
Senha SMTP	
Porta SMTP	25 (Valor padrão)
E-mail de onde as notificações de alerta são enviadas	
Nome do host ou endereço IP do servidor de autenticação	
Nome do administrador do Active Directory ou nome distinto do vínculo LDAP	
Senha do Active Directory ou senha de vinculação LDAP	
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 da armadilha SNMP	
Porta SNMP	

Informações do cluster

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

Cluster 1 de N	Seu valor
Nome do host ou endereço IP de gerenciamento de cluster	

Cluster 1 de N	Seu valor
Nome de usuário do administrador ONTAP  O administrador deve ter recebido a função "admin".	
Senha do administrador do ONTAP	
Protocolo	HTTPS

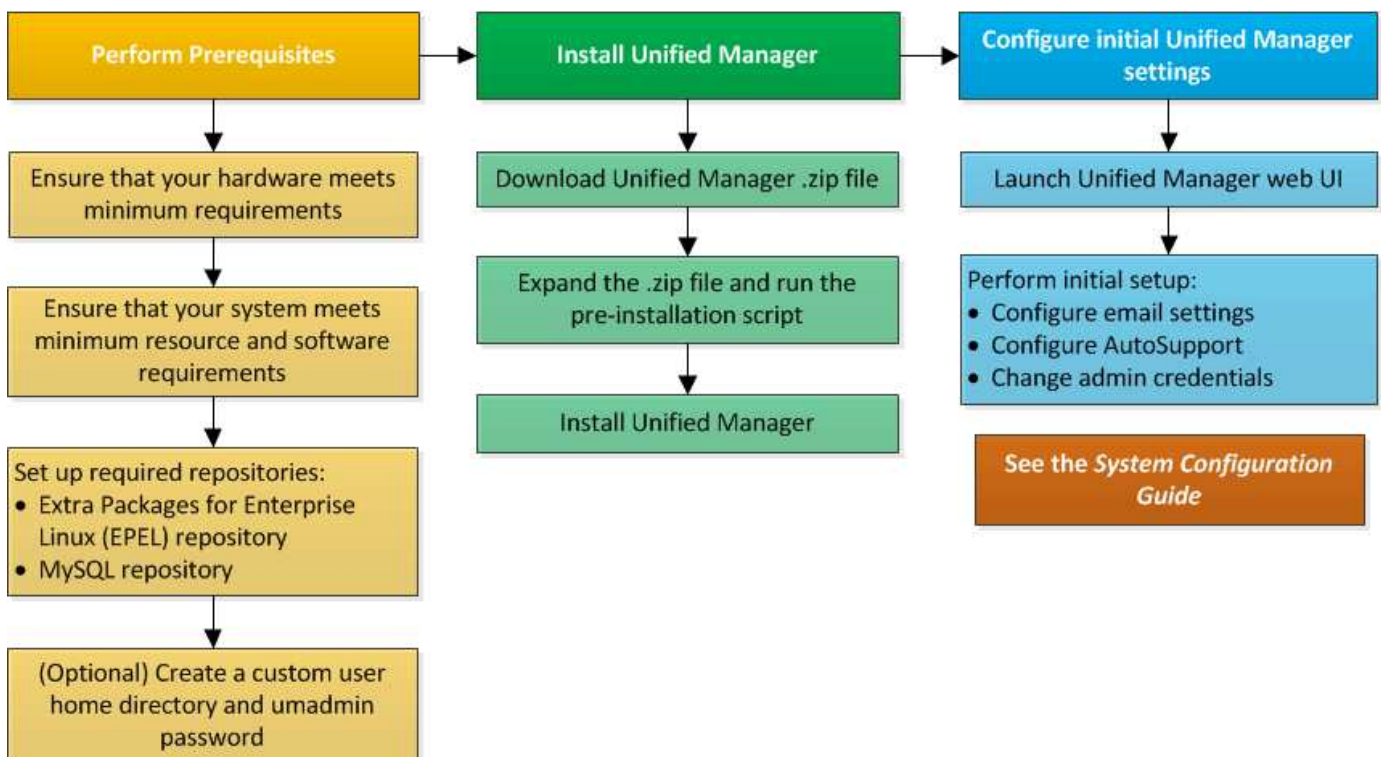
Instalar, atualizar e remover o software Unified Manager

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 estar sendo executado em uma máquina física ou em uma máquina virtual executada 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 poder usar o Unified Manager.



Configurar 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.

Configurar manualmente o repositório EPEL

Se o sistema no qual você está instalando o Unified Manager não tiver acesso ao repositório Extra Packages for Enterprise Linux (EPEL), 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. Use 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, baixe-a em:

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

Para a versão 9, baixe-a 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 dos pacotes modulares também estejam disponíveis no mesmo repositório.

Configurar 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 no seu sistema.



Esta tarefa pode falhar se o sistema não tiver conectividade com a 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, baixe-a em:

```
wget http://repo.mysql.com/yum/mysql-8.4-community/el/8/x86_64/mysql84-community-release-el8-1.noarch.rpm
```

Para a versão 9, baixe-a em:

```
wget http://repo.mysql.com/yum/mysql-8.4-community/el/9/x86_64/mysql84-community-release-el9-1.noarch.rpm
```

2. Configure o repositório MySQL:

```
yum install mysql84-community-release-.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, será necessário desabilitar 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 de chave ausente ou incompatibilidade de chave e sua 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-2023
```

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

Requisitos do SELinux em compartilhamentos NFS e CIFS

Se você está planejando montar `/opt/netapp` ou `/opt/netapp/data` em um dispositivo NAS ou SAN e você 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 se você tiver 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 definir e confirmar o contexto correto do SELinux.

Configurar o contexto SELinux quando `/opt/netapp/data` está montado

Se você montou `/opt/netapp/data` no seu sistema e o SELinux está definido para `Enforcing`, certifique-se de que o tipo de contexto SELinux para `/opt/netapp/data` está definido para `mysqld_db_t`, que é o elemento de contexto padrão para o local dos arquivos de banco de dados.

1. Execute este comando para verificar o contexto:

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

Um exemplo de saída:

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



Nesta saída, o contexto é `default_t`. Você deve mudar este 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 para `mysqld_db_t`:

```
semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"
`restorecon -R -v /opt/netapp/data
```
 - b. Se você configurou `/opt/netapp/data` em `/etc/fstab`, você deve editar o `/etc/fstab` arquivo. Para o `/opt/netapp/data/` opção de montagem, adicione o rótulo MySQL como:

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

- c. Desmontar e remontar `/opt/netapp/data/` para habilitar o contexto.
- d. Se você tiver uma montagem NFS direta, execute o seguinte comando para definir o contexto para `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/
```

Um exemplo de saída:

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

Configurar o contexto SELinux quando `/opt/netapp` é montado, e `/opt/netapp/data/` também é montado separadamente

Neste cenário, em primeiro lugar, você deve definir o contexto para `/opt/netapp/data/` conforme 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
```

Um exemplo de saída:

```
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 para `usr_t`. Você pode definir o contexto para qualquer valor diferente de `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`.
 - a. Execute os seguintes comandos para definir o contexto:

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

1. Se você configurou `/opt/netapp` em `/etc/fstab`, você deve editar o `/etc/fstab` arquivo. Para o `/opt/netapp` opção de montagem, adicione o rótulo MySQL como:

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

2. Desmonte e monte novamente `/opt/netapp` para habilitar 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
```

Configurar o contexto SELinux quando `/opt/netapp` é montado, e `/opt/netapp/data/` não é montado separadamente

Se você montou `/opt/netapp` no seu sistema e o SELinux está definido para `Enforcing`, certifique-se de que o tipo de contexto SELinux para `/opt/netapp` está definido para `mysqld_db_t`, que é o elemento de contexto padrão para o local dos arquivos de banco de dados.

Passos

1. Execute este comando para verificar o contexto:

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

Um exemplo de saída:

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



Nesta saída, o contexto é `default_t`. Você deve mudar este contexto para `mysqld_db_t`.

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

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

```
semanage fcontext -a -t mysqld_db_t "/opt/netapp"  
`restorecon -R -v /opt/netapp
```
- Se você configurou `/opt/netapp` em `/etc/fstab`, edite o `/etc/fstab` arquivo. Para o `/opt/netapp/` opção de montagem, adicione o rótulo MySQL como:

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

Um exemplo de saída:

```
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 seu cenário de instalação.

Crie um diretório inicial de usuário personalizado e uma senha de administrador antes da instalação

Você pode criar um diretório inicial personalizado e definir sua própria senha de usuário `umadmin` antes de instalar o Unified Manager. Esta 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 atender aos requisitos descritos em "[Requisitos do sistema de hardware](#)".
- Você deve conseguir efetuar login como usuário `root` 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 inicial.
- Atribui a senha padrão “admin” ao usuário `umadmin`.

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

Se o seu 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 da 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, você deverá adicioná-lo novamente. Você precisa preservar a configuração do `sudoers` porque algumas operações do Unified Manager exigem esses privilégios de `sudo`.

As políticas de segurança em seu ambiente não devem restringir privilégios `sudo` para o usuário de manutenção do Unified Manager. Algumas operações do Unified Manager podem falhar se os privilégios forem restritos. Verifique se você consegue executar o seguinte comando `sudo` quando estiver conectado como 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. Efetue login como usuário `root` no servidor.
2. Crie a conta do grupo `umadmin` chamada “maintenance”:

```
groupadd maintenance
```

3. Crie a conta de usuário “`umadmin`” no grupo de manutenção em um diretório inicial 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 senha para o usuário `umadmin`.

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

Baixar o Unified Manager

Você deve baixar o Unified Manager .zip arquivo do site de suporte da NetApp para instalar o Unified Manager.

Antes de começar

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

Baixe o pacote de instalação do Unified Manager para o sistema Red Hat Enterprise Linux.

Passos

1. Efetue login no site de suporte da NetApp e navegue até a página de download do Unified Manager:

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

2. Selecione a versão necessária do Unified Manager e aceite o contrato de licença de usuário final (EULA).
3. Baixe o arquivo de instalação do Unified Manager para Linux e salve-o .zip arquivo para um diretório no sistema de destino.



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

4. Verifique a soma de verificação para integridade do software baixado.
5. Se você baixou 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 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 para uso.

Instalar o Unified Manager

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

Antes de começar

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

Ver"Requisitos do sistema de hardware" .

Ver"Requisitos de instalação e software Linux" .

- Você deve ter baixado o Unified Manager .zip arquivo do site de suporte da NetApp para o sistema de destino.
- Você deve ter verificado a integridade do arquivo baixado .zip arquivo.
- Você deve ter um navegador da web compatível.
- Seu software de emulação de terminal deve ter o scrollbar habilitado.

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

Passos

1. Efetue login no servidor no qual você está instalando o Unified Manager.
2. Insira os comandos apropriados para avaliar qual software pode exigir instalação ou atualização no sistema de destino para dar suporte à instalação:

Software necessário e versão mínima	Comando para verificar software e versão
OpenJDK versão 11.0.25	<code>java -version</code>
MySQL 8.4.4 Edição Comunitária	<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 8.4.4 Community Edition, digite o seguinte comando para desinstalá-lo:

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

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

4. Navegue até o diretório onde você baixou a instalação .zip arquivo e expanda o pacote do Unified Manager:

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

O necessário .rpm Os módulos do Unified Manager são descompactados no 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 do 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 tem acesso aos repositórios de software necessários. Se o script identificar algum problema, você deverá corrigi-lo 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 desabilitar seu 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 a etapa 7 somente se o seu sistema não estiver conectado à Internet e você tiver que baixar manualmente os pacotes necessários para sua instalação. Se o seu sistema tiver acesso à Internet e todos os pacotes necessários estiverem disponíveis, vá para a etapa 8. Para sistemas que não estão conectados à Internet ou que não estão usando os repositórios do Red Hat Enterprise Linux, execute as seguintes etapas para determinar se está faltando algum pacote necessário e, em seguida, baixe esses pacotes:

- a. No sistema em que você está instalando o Unified Manager, visualize 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 com acesso à Internet, baixe os pacotes que faltam:

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



Como o plug-in “yum-plugin-downloadonly” nem sempre está habilitado em sistemas Red Hat Enterprise Linux, talvez seja necessário 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 seu sistema de instalação.

8. Como usuário root, 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 uma URL:

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2023
```



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 por e-mail exibida imediatamente após as mensagens de instalação.

O e-mail notifica o usuário root sobre uma falha inicial na tarefa cron, que não tem efeito adverso na instalação.

10. Após a conclusão das mensagens de instalação, role para trás pelas mensagens até ver a mensagem na qual o sistema exibe um endereço IP ou URL para a interface de usuário da Web do Unified Manager, o nome de 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, deverá especificar o shell de login do usuário umadmin:

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

Acesse a interface 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 efetuar login no Unified Manager pela primeira vez. Este usuário recebe a função de usuário "Administrador de Aplicativos" e é configurado como o tipo "Usuário de Manutenção". Este usuário foi criado pelo Unified Manager.

- **jboss**

Usado para executar serviços do Unified Manager relacionados ao utilitário JBoss. Este usuário foi 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: manutenção, 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 do 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 root ao sistema Red Hat Enterprise Linux no qual o Unified Manager está instalado.
- Você deve ser capaz de acessar o NetApp fornecido `password.sh` script no diretório `/opt/netapp/essentials/bin`.

Passos

1. Efetue login como usuário root no sistema.
2. Pare os serviços do Unified Manager inserindo os seguintes comandos na ordem mostrada:

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

Não interrompa 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, em seguida, digite-a uma segunda vez para confirmação.

Observe que a senha deve ter entre 8 e 16 caracteres e deve conter pelo menos um dígito, uma letra maiúscula e uma minúscula e pelo menos um destes 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 efetuar login na interface do usuário do Unified Manager.

Atualizar o 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 pela NetApp, são instaladas usando o mesmo procedimento das novas versões.

Se o Unified Manager estiver pareado com uma instância do OnCommand Workflow Automation e houver novas versões de software disponíveis para ambos os produtos, você deverá desconectar os dois produtos e configurar uma nova conexão do Workflow Automation após executar as atualizações. Se você estiver realizando uma atualização para apenas um dos produtos, faça login no Workflow Automation após a atualização e verifique se ele ainda está adquirindo dados do Unified Manager.

Caminho de atualização com suporte para versões do Unified Manager

O Active IQ Unified Manager oferece suporte a um caminho de atualização específico para cada versão.

Nem todas as versões do Unified Manager podem executar uma atualização local para versões posteriores. As atualizações do Unified Manager são limitadas a um modelo N-2, o que significa que uma atualização só pode ser realizada nas próximas 2 versões em todas as plataformas. Por exemplo, você pode executar uma atualização do Unified Manager 9.16 somente a partir 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 para uma das versões suportadas primeiro e depois atualizada para a versão atual.

Por exemplo, se a sua versão instalada for o Unified Manager 9.9 e você quiser atualizar para o Unified Manager 9.14, siga uma sequência de atualizações.

Caminho de atualização de exemplo:

1. Atualização 9.11 → 9.13
2. Atualização 9.13 → 9.14
3. Atualização 9.13 → 9.16
4. Atualização 9.14 → 9.16

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

Atualizar o Unified Manager

Você pode atualizar do Unified Manager 9.13 ou 9.14 para o 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.

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

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

- Você deve 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.

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

- Para evitar perda de dados, você deve ter criado um backup do banco de dados do Unified Manager caso haja algum problema durante a atualização. A 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 retenção de dados de desempenho por 13 meses ou alterá-las para 6 meses. Após a confirmação, os dados de desempenho histórico são eliminados após 6 meses.
- Você deve ter concluído todas as operações em execução, porque o Unified Manager não estará 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 8.4.4, o processo de atualização do Unified Manager atualizará automaticamente o MySQL para a 8.4.4.

Passos

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

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

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 haja configurações do 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 tem acesso aos repositórios de software necessários. Se o script identificar algum problema, você deverá corrigi-lo e continuar com a atualização.

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

6. Atualize o Unified Manager usando o seguinte script:

```
upgrade.sh
```

Este script executa automaticamente os módulos RPM, atualizando o software de suporte necessário e os módulos do Unified Manager executados neles. Além disso, o script de atualização verifica se há alguma configuração do sistema ou algum software instalado que possa entrar em conflito com a atualização. Se o script identificar algum problema, você deverá corrigi-lo antes de atualizar o Unified Manager. Se você tiver instalado pacotes anteriormente, como *net-snmp*, antes de atualizar o Unified Manager, a dependência do MySQL poderá desinstalar o pacote durante a atualização. Você precisa instalar o pacote manualmente novamente para continuar a usá-lo.

7. Após a conclusão da atualização, role as mensagens até ver a mensagem exibindo um endereço IP ou URL para a interface de usuário 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 interface de usuário da Web do Unified Manager e, em seguida, faça login usando o mesmo nome de usuário de manutenção (umadmin) e senha que você definiu anteriormente.

Etapas adicionais a serem executadas para pacotes ausentes

Se houver algum pacote ausente detectado no seu site durante a atualização, ou se o seu sistema não estiver conectado à Internet, ou se você não estiver usando os repositórios do Red Hat Enterprise Linux, execute as seguintes etapas para determinar se há algum pacote necessário ausente e baixe-o.



Essas 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 tenha acesso à Internet, execute o seguinte comando para baixar os pacotes ausentes.

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

Os pacotes são baixados no diretório especificado como `--downloadaddir=.`

Como o plug-in “yum-plugin-downloadonly” nem sempre está habilitado em sistemas Red Hat Enterprise Linux, talvez seja necessário habilitar a funcionalidade para baixar um pacote sem instalá-lo:

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

3. Copie os pacotes baixados para o diretório onde você descompactou o pacote do Unified Manager no sistema de instalação.
4. Mude 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
```

Este 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 interface de usuário da Web do Unified Manager e, em seguida, faça login usando o mesmo nome de usuário de manutenção (umadmin) e senha que você definiu anteriormente.

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

Se você instalou anteriormente 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 esta 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 possível. Lacunas nos dados coletados aparecem na interface do usuário do Unified Manager durante o período em que o sistema Red Hat Enterprise Linux 7.x é desligado e antes do novo Red Hat Enterprise Linux 8.x ser iniciado.

Ver ["Gerenciando operações de backup e restauração"](#) se você precisar revisar instruções detalhadas para os processos de backup e restauração.

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

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

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 existente.

Ver ["Instalando o Unified Manager no Linux"](#) .

Não inicie a interface do usuário nem configure nenhum cluster, usuário ou configuração 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 Administração na interface da web, crie um backup do Unified Manager e copie o arquivo de backup(.7z arquivo) e o conteúdo do diretório do repositório do banco de dados(/database-dumps-repo subdiretório) para um local externo.
4. No sistema Red Hat Enterprise Linux 7.x, desligue o Unified Manager.
5. No sistema Red Hat Enterprise Linux 8.x, copie o arquivo de backup(.7z arquivo) do local externo para /opt/netapp/data/ocum-backup/ e os arquivos do repositório de 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 seu navegador para iniciar a interface de usuário 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 host no mesmo servidor

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

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

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

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.

Ver ["Instalando o Unified Manager no Linux"](#) .

Não inicie a interface do usuário nem configure nenhum cluster, usuário ou configuração de autenticação quando a instalação estiver concluída. O arquivo de backup preenche essas informações durante o processo de restauração.

5. Copie o arquivo de backup(. 7z arquivo) do local externo para /opt/netapp/data/ocum-backup/ e os arquivos do repositório de 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 seu navegador para iniciar a interface de usuário da web do Unified Manager e, em seguida, faça login no sistema.

Atualizar produtos de terceiros após a instalação do Unified Manager

Você pode atualizar produtos de terceiros, como o 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 conforme sua própria programação.

Atualizar 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 deve ter privilégios de root para o sistema Linux no qual o Unified Manager está instalado.

Você pode atualizar versões do OpenJDK dentro de famílias de versões. 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. Efetue login como usuário root 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
```

Reiniciar o Unified Manager

Talvez seja necessário reiniciar o Unified Manager após fazer alterações na configuração.

Antes de começar

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

Passos

1. Efetue login como usuário root no servidor no qual 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.

Remover o 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 root ao servidor do qual deseja remover o Unified Manager.
- O Security-Enhanced Linux (SELinux) deve ser desabilitado no sistema Linux. Altere o modo 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 3306 do MySQL. As regras de firewall não são excluídas automaticamente.

Passos

1. Efetue login como usuário root no servidor do 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 NetApp RPM associados. Ele não remove os módulos de software pré-requisitos, 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 será removido. Todos os dados do `/opt/netapp/data` diretório é movido para o `/opt/netapp/data/BACKUP` pasta após a desinstalação. Desinstalar o Unified Manager também remove os pacotes Java e MySQL, a menos que os pacotes sejam necessários e usados por qualquer outro aplicativo no sistema. Entretanto, os dados do MySQL não são excluídos.

Remover o usuário umadmin personalizado 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 um usuário umadmin definido personalizado e uma conta de manutenção. Você deve excluir esses itens manualmente.

Passos

1. Efetue login como usuário root no servidor Red Hat Enterprise Linux.
2. Exclua o usuário umadmin:

```
userdel umadmin
```

3. Excluir o grupo de manutenção:

```
groupdel maintenance
```

Instalar o Unified Manager em sistemas Windows

Introdução ao Active IQ Unified Manager

O Active IQ Unified Manager (antigo OnCommand Unified Manager) permite que você monitore e gerencie a integridade e o desempenho dos seus sistemas de armazenamento ONTAP a partir de 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, a disponibilidade, a proteção e o status de desempenho dos sistemas de armazenamento monitorados.

Informações relacionadas

["Ferramenta de Matriz de Interoperabilidade da NetApp"](#)

O que o servidor Unified Manager faz

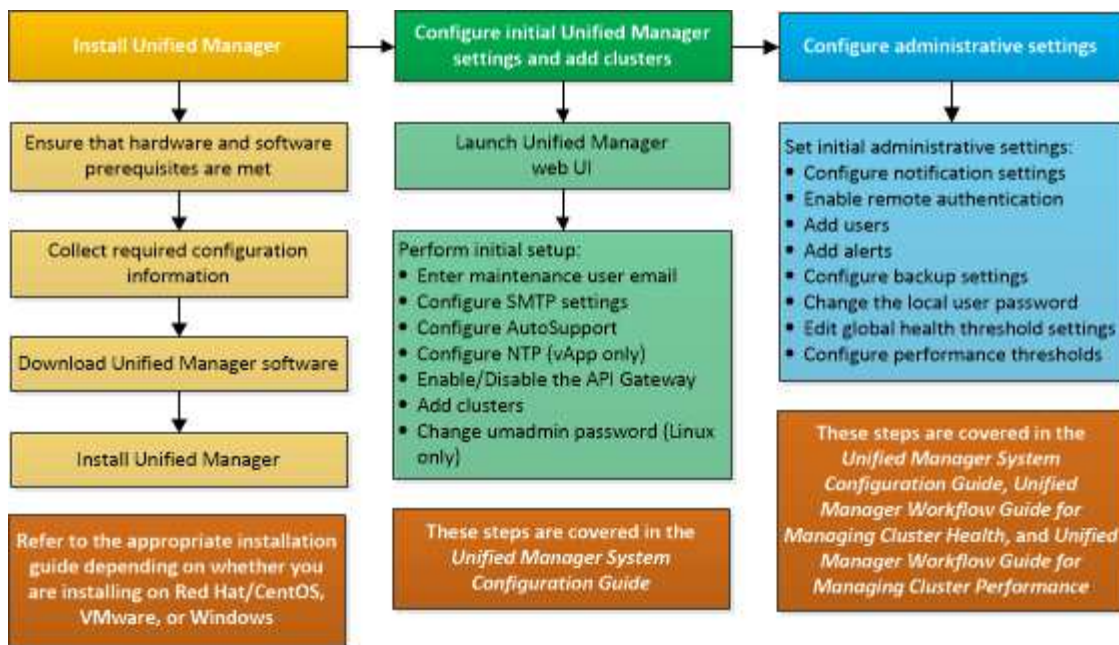
A infraestrutura do servidor do Unified Manager consiste em uma unidade de coleta de dados, um banco de dados e um servidor de aplicativos. Ele fornece serviços de infraestrutura, como descoberta, monitoramento, controle de acesso baseado em funções (RBAC), auditoria e registro.

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

Visão geral da sequência de instalação

O fluxo de trabalho de instalação descreve as tarefas que você deve executar antes de poder 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, certifique-se de que 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 Unified Manager. Se precisar aplicar quaisquer medidas de segurança ao servidor do Unified Manager, você deverá fazer 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 Conhecimento.

["Suportabilidade para medidas de segurança aplicadas ao Active IQ Unified Manager para Data ONTAP"](#)

Informações relacionadas

["Ferramenta de Matriz de Interoperabilidade da 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 a níveis de desempenho aceitáveis.

Configuração de hardware	Configurações recomendadas
BATER	12 GB (requisito mínimo de 8 GB)
Processadores	4 CPUs

Configuração de hardware	Configurações recomendadas
Capacidade do ciclo da CPU	9572 MHz total (requisito mínimo 9572 MHz)
Espaço livre em disco	150 GB, onde a capacidade é alocada da seguinte forma: • 100 GB de espaço em disco para o diretório de instalação • 50 GB de espaço em disco para o diretório de dados MySQL

O Unified Manager pode ser instalado em sistemas com pouca memória, mas os 12 GB de RAM recomendados garantem que haja memória suficiente disponível para um desempenho ideal e para que o sistema possa acomodar clusters e objetos de armazenamento adicionais conforme sua configuração cresce. Você não deve definir nenhum limite de memória na VM onde o Unified Manager está implantado e não deve habilitar nenhum recurso (por exemplo, balão) que impeça 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 você instalar uma segunda instância do Unified Manager. Para mais informações, consulte o *Guia de Melhores Práticas*.

["Relatório Técnico 4621: Guia de Melhores Práticas do Unified Manager"](#)

A troca de páginas de memória afeta negativamente o desempenho do sistema e do aplicativo de gerenciamento. Competir por recursos de CPU que não estão disponíveis devido à utilização geral do host pode prejudicar o desempenho.

Requisito de 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. Outros aplicativos podem consumir recursos do sistema e reduzir drasticamente o desempenho do Unified Manager.

Requisitos de espaço para backups

Se você planeja usar o recurso de backup e restauração do Unified Manager, aloque capacidade adicional para que o diretório ou disco “data” tenha 150 GB de espaço. Um backup pode ser gravado em um destino local ou 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 do host

O sistema físico ou virtual no qual você instala o Unified Manager deve ser configurado de forma que você possa `ping` o nome do host do próprio host. No caso de configuração IPv6, você deve verificar se `ping6` para o nome do host for 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 interface da web do produto. Se você configurou um endereço IP estático para sua rede durante a implantação, você designou um nome para o host da rede. Se você configurou a rede usando DHCP, deverá obter o nome do host do DNS.

Se você planeja permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o

nome de domínio totalmente qualificado (FQDN) ou endereço IP, sua configuração de rede precisa 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 operacional

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 atualizada de versões do Windows suportadas.

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



A NetApp não oferece suporte à instalação do Unified Manager usando ferramentas de terceiros, como o Microsoft System Center Configuration Manager (SCCM).

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 no seu sistema Windows devido a regulamentações da empresa. Você deve desabilitar o software antivírus antes de instalar o Unified Manager para evitar que a instalação falhe.

Software de terceiros

Os seguintes pacotes de terceiros estão incluídos no Unified Manager. Se esses pacotes de terceiros não estiverem instalados no seu sistema, o Unified Manager os instalará como parte da instalação.

- Pacotes redistribuíveis do Microsoft Visual C para Visual Studio 2015 versão 14.26.28720.3
- MySQL Community Edition versão 8.4.4
- Python 3.12.4
- OpenJDK versão 11.0.25
- 7-zip 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 mais 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 “MYSQL84”.

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



Você deve desligar uma instância em execução do Unified Manager antes de atualizar qualquer software de terceiros. Após a conclusão da instalação do software de terceiros, você pode reiniciar o Unified Manager.

Requisitos de instalação

- O Microsoft .NET 4.5.2 ou superior deve ser instalado.
- O `temp` O 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 forma que `ping` as respostas ao nome do host e ao FQDN são bem-sucedidas.
- Você deve desabilitar o serviço de publicação na Web do Microsoft IIS e garantir que as portas 80 e 443 estejam livres.
- Você deve certificar-se de que a configuração do Host de Sessão da Área de Trabalho Remota para “Compatibilidade com RDS do Windows Installer” esteja desabilitada durante a instalação.
- A porta UDP 514 deve estar livre e não deve ser usada por nenhum outro serviço.
- Você deve desabilitar todos os softwares antivírus no 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 interface da Web do Unified Manager, use um navegador compatível.

A Matriz de Interoperabilidade tem a lista de versões de navegadores suportadas.

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

Para todos os navegadores, desabilitar os bloqueadores de 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, verifique também a lista de navegadores suportados pelo IdP.

Requisitos de protocolo e porta

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

Conexões com o servidor do Unified Manager

Em instalações típicas, você não precisa especificar números de porta ao se conectar à interface de usuário 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 inserir `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
Interface da Web do Unified Manager	HTTP	80	Usado para acessar a interface da web do Unified Manager; redireciona automaticamente para a porta segura 443.
Interface da Web do Unified Manager e programas que usam APIs	HTTPS	443	Usado para acessar com segurança a interface da Web do Unified Manager ou para fazer chamadas de API; chamadas de API só podem ser feitas usando HTTPS.
Console de manutenção	SSH/SFTP	22	Usado para acessar o console de manutenção e recuperar pacotes de suporte.
Linha de comando do Linux	SSH/SFTP	22	Usado para acessar a linha de comando do Red Hat Enterprise Linux e recuperar pacotes de suporte.

Interface	Protocolo	Porta	Descrição
Log de sistema	UDP	514	Usado para acessar mensagens EMS baseadas em assinatura de sistemas ONTAP e para criar eventos com base nas mensagens.
DESCANSAR	HTTPS	9443	Usado para acessar eventos EMS baseados em API REST em tempo real de sistemas ONTAP autenticados.
Banco de dados MySQL	MySQL	3306	Usado para habilitar o acesso do OnCommand Workflow Automation e do OnCommand API Services ao Unified Manager.
Corretor AMQP QPID	TCP/IP	56072	Usado para comunicação de mensagens internas.
Corretor AMQP QPID	WebSocket sobre TCP	56080	Usado para escutar nesta porta mensagens recebidas do ONTAP (agente de nuvem).
Corretor AMQP QPID	WebSocket sobre TCP	56443	Usado para escutar nesta porta mensagens recebidas do ONTAP (agente de nuvem). A comunicação por esta porta suporta criptografia fornecida por TLS ou SSL.



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

Conexões do servidor do Unified Manager

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

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

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

Destino	Protocolo	Porta	Descrição
Sistema de armazenamento	HTTPS	443/TCP	Usado para monitorar e gerenciar sistemas de armazenamento.
Sistema de armazenamento	NDMP	10000/TCP	Usado para determinadas operações de restauração de Snapshot.
Servidor AutoSupport	HTTPS	443	Usado para enviar informações do AutoSupport . É necessário 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 e-mail
SMTP	25	Usado para enviar e-mails de notificação de alerta.	Remetente de armadilha SNMP
SNMPv1 ou SNMPv3	162/UDP	Usado para enviar notificações de alerta de traps SNMP.	Servidor provedor de dados externo
TCP	2003	Usado para enviar dados de desempenho para um provedor de dados externo, como o Graphite.	Servidor NTP

Destino	Protocolo	Porta	Descrição
NTP	123/UDP	Usado para sincronizar o horário no servidor do Unified Manager com um servidor de horário NTP externo. (Somente sistemas VMware)	Corretor AMQP QPID
TCP/IP	56072	Usado para comunicação de mensagens internas.	Corretor AMQP QPID
WebSocket sobre TCP	56080	Usado para escutar nesta porta mensagens recebidas do ONTAP (agente de nuvem).	Corretor AMQP QPID
WebSocket sobre TCP	56443	Usado para escutar nesta porta mensagens recebidas do ONTAP (agente de nuvem). A comunicação por meio desta porta suporta criptografia fornecida por TLS ou SSL.	Log de sistema

Complete a planilha

Antes de instalar e configurar o Unified Manager, você deve ter informações específicas sobre seu ambiente prontamente disponíveis. Você pode registrar as informações na planilha.

Informações de instalação do Unified Manager

Os detalhes necessários para instalar o Unified Manager.

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

Sistema no qual o software é implantado	Seu valor
Endereço DNS secundário	
Domínios de pesquisa	
Nome de usuário de manutenção	
Senha do usuário de manutenção	

Informações de configuração do Unified Manager

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

Contexto	Seu valor
Endereço de e-mail do usuário de manutenção	
Nome do host ou endereço IP do servidor SMTP	
Nome de usuário SMTP	
Senha SMTP	
Porta SMTP	25 (Valor padrão)
E-mail de onde as notificações de alerta são enviadas	
Nome do host ou endereço IP do servidor de autenticação	
Nome do administrador do Active Directory ou nome distinto do vínculo LDAP	
Senha do Active Directory ou senha de vinculação LDAP	
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 da armadilha SNMP	

Contexto	Seu valor
Porta SNMP	

Informações do cluster

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

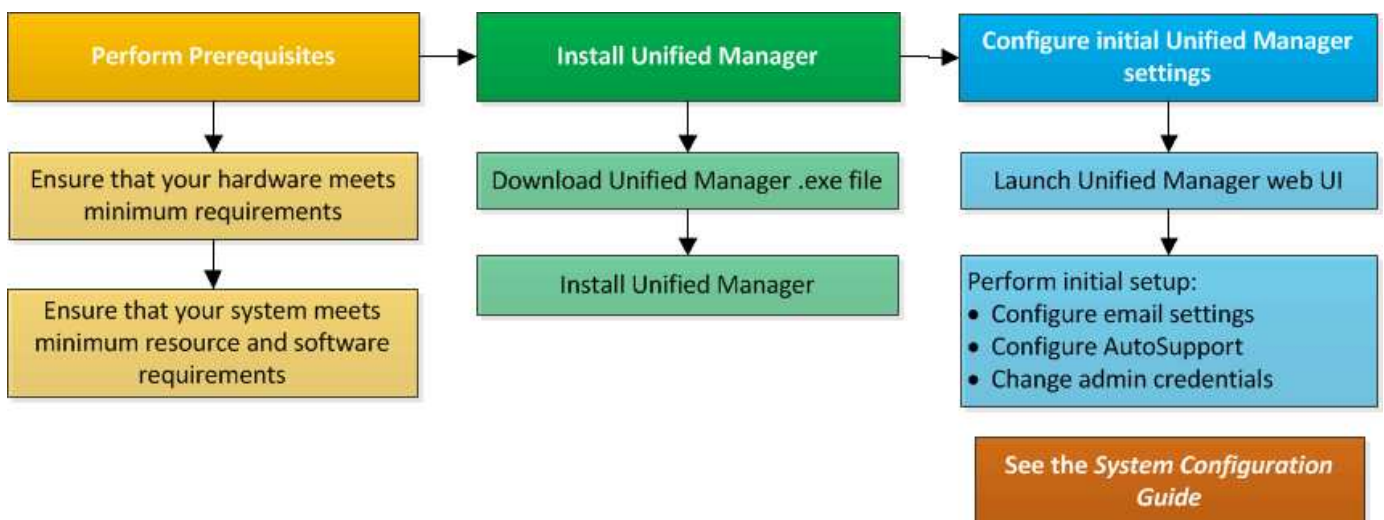
Cluster 1 de N	Seu valor
Nome do host ou endereço IP de gerenciamento de cluster	
Nome de usuário do administrador ONTAP  O administrador deve ter recebido a função "admin".	
Senha do administrador do ONTAP	
Protocolo	HTTPS

Instalar, atualizar e remover o 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 poder 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

Você pode instalar o Unified Manager para monitorar e solucionar problemas de capacidade de armazenamento de dados, disponibilidade, desempenho e proteção.

Antes de começar

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

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

Ver ["Requisitos de software e instalação do Windows"](#) .



A partir do Unified Manager 9.5, o OpenJDK é fornecido no pacote de instalação e instalado automaticamente. O Oracle Java não é mais suportado a partir do Unified Manager 9.5.

- Você deve ter privilégios de administrador do Windows. Certifique-se de que seu nome de usuário não comece 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 suportados, exceto os 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, conter letras maiúsculas ou minúsculas, numerais e caracteres especiais.
- Os seguintes caracteres especiais não são permitidos na sequência de senha do usuário de manutenção ou do usuário root do MySQL: " ' ` % , = & < > | ^ \ / () [] ; :

Os seguintes caracteres especiais são permitidos: ~ ! @ # \$ % ^ & * - ? . + { }

Passos

1. Efetue login no Windows usando a conta de administrador local padrão.
2. Efetue login no site de suporte da NetApp e navegue até a página de download do Unified Manager:

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

3. Selecione a versão necessária do Unified Manager e aceite o contrato de licença de usuário final (EULA).
4. Baixe o arquivo de instalação do Unified Manager para Windows ou o arquivo 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 mouse e execute o arquivo executável (.exe) do instalador do Unified Manager como administrador.

O Unified Manager detecta 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 **Avançar**.
8. Digite o nome de usuário e a senha para criar o usuário de manutenção.
9. No assistente de conexão de banco de dados, insira a senha root do MySQL.
10. Clique em **Alterar** para especificar um novo local para o diretório de instalação do Unified Manager e o diretório de dados do MySQL.

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

11. Clique em **Avançar**.
12. No assistente Pronto para instalar o Shield, clique em **Instalar**.
13. Após a conclusão da instalação, clique em **Concluir**.
14. Se você 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 Unified Manager (appDataDir)

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

C:\ProgramData\NetApp\OnCommandAppData\

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

Executar uma instalação autônoma do Unified Manager

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

Passos

1. Efetue login na interface de linha de comando do Windows usando a conta de administrador local padrão.
2. Navegue até o local onde deseja instalar o Unified Manager e escolha uma das seguintes opções:

Opção	Instruções
Se 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_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qn /l*v CompletePathForLogFile"</pre> Exemplo: <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>
Se os 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"</pre> Exemplo: <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 /qr /l*v C:\install.log"</pre>

O /qr opção ativa o modo silencioso com uma interface de usuário reduzida. Uma interface de usuário básica é exibida, mostrando o progresso da instalação. Não serão solicitadas entradas. Se pacotes de terceiros como JRE, MySQL e 7zip não estiverem pré-instalados, você deve usar o /qr opção. A instalação falha se o /qn A opção é usada em um servidor onde pacotes de terceiros não estão instalados.

O `/qn` opção ativa o modo silencioso sem interface de usuário. Nenhuma interface de usuário ou detalhes são exibidos durante a instalação. Você não deve usar o `/qn` opção quando pacotes de terceiros não estão instalados.

3. Efetue 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 do 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 privilégios de administrador do Windows para o sistema no qual o Unified Manager está instalado.
- Você deve ter a senha do usuário root do MySQL.
- Você deve conseguir acessar o NetApp fornecido `password.bat` script no diretório

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

Passos

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

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

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

Observe que a senha deve ter entre 8 e 16 caracteres e deve conter pelo menos um dígito, uma letra maiúscula e uma minúscula e pelo menos um destes caracteres especiais:

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

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

Caminho de atualização com suporte para versões do Unified Manager

O Active IQ Unified Manager oferece suporte a um caminho de atualização específico para cada versão.

Nem todas as versões do Unified Manager podem executar uma atualização local para versões posteriores. As atualizações do Unified Manager são limitadas a um modelo N-2, o que significa que uma atualização só pode ser realizada nas próximas 2 versões em todas as plataformas. Por exemplo, você pode executar uma atualização do Unified Manager 9.16 somente a partir 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 para uma das versões suportadas primeiro e depois atualizada para a versão atual.

Por exemplo, se a sua versão instalada for o Unified Manager 9.9 e você quiser atualizar para o Unified Manager 9.14, siga uma sequência de atualizações.

Caminho de atualização de exemplo:

1. Atualização 9.11 → 9.13
2. Atualização 9.13 → 9.14
3. Atualização 9.13 → 9.16
4. Atualização 9.14 → 9.16

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

Atualizar o Unified Manager

Você pode atualizar o Unified Manager 9.13 ou 9.14 para o 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.

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

Ver ["Requisitos de software e instalação do Windows"](#).



A partir do Unified Manager 9.5, o OpenJDK é fornecido no pacote de instalação e instalado automaticamente. O Oracle Java não é mais 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 8.4.4, o processo de atualização do Unified Manager atualizará automaticamente o MySQL para a 8.4.4. Você não deve executar uma atualização autônoma de uma versão anterior do MySQL para 8.4.4.
- Todos os clusters são suportados, exceto os sistemas ASA r2.
- Você deve ter privilégios de administrador do Windows. Certifique-se de que seu nome de usuário não

comece 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 efetuar login no site de suporte da NetApp .
- Para evitar 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 que o tamanho do diretório de dados. A atualização é interrompida e exibe uma mensagem de erro indicando a quantidade de espaço a ser adicionado caso não haja espaço livre suficiente.

- Durante a atualização, você pode ser solicitado a confirmar se deseja manter as configurações padrão anteriores para retenção de dados de desempenho por 13 meses ou alterá-las para 6 meses. Após a confirmação, os dados históricos de desempenho após 6 meses são eliminados.
- Antes de atualizar, você deve fechar todos os arquivos ou pastas abertos em *<InstallDir>\JDK* e *MySQL Data Directory*.
- Se você tiver um software antivírus ativo instalado no seu sistema Windows, a atualização do Unified Manager poderá falhar. Você deve desabilitar todos os softwares antivírus no seu sistema antes de atualizar o Unified Manager.

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

Se o Unified Manager estiver pareado com uma instância do OnCommand Workflow Automation e houver novas versões de software disponíveis para ambos os produtos, você deverá desconectar os dois produtos e configurar uma nova conexão do Workflow Automation após executar as atualizações. Se você estiver realizando uma atualização para apenas um dos produtos, faça login no Workflow Automation após a atualização e verifique se ele ainda está adquirindo dados do Unified Manager.

Passos

1. Efetue login no site de suporte da NetApp e navegue até a página de download do Unified Manager:

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

2. Selecione a versão necessária do Unified Manager e aceite o contrato de licença de usuário final (EULA).
3. Baixe o arquivo de instalação do Unified Manager para Windows ou o arquivo 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 mouse e execute o arquivo executável (.exe) do instalador do Unified Manager como administrador.

O Unified Manager exibe a seguinte mensagem:

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

4. Clique em **Sim** e depois em **Avançar**.
5. Digite a senha root do MySQL84 que foi definida durante a instalação e clique em **Avançar**.
6. Inicie a interface 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 você tiver um software antivírus ativo instalado no seu 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"`

Atualizar produtos de terceiros

Você pode atualizar produtos de terceiros, como o 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 conforme sua própria programação.

Atualizar o OpenJDK

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

Antes de começar

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

Você pode atualizar versões do OpenJDK dentro de famílias de versões. 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. Efetue login como usuário administrador na máquina host do Unified Manager.
2. Baixe a versão apropriada do OpenJDK (64 bits) do site do OpenJDK para o sistema de destino.

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



É necessária uma conta Oracle para baixar o arquivo. Se você não tiver uma conta Oracle, vá para "[Login na conta Oracle](#)" página para criar uma.

3. Use o console de Serviços do Windows para interromper os seguintes serviços do Unified Manager:
 - Serviço de aquisição NetApp Active IQ (Ocie-au)
 - Serviço de servidor de gerenciamento NetApp Active IQ (Oncommandsvc)
4. Expandir o zip arquivo.

5. Copie os diretórios e arquivos do resultado jdk diretório (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 de Serviços do Windows:
 - Serviço de servidor de gerenciamento NetApp Active IQ (Oncommandsvc)
 - Serviço de aquisição NetApp Active IQ (Ocie-au)

Desinstalar produtos de terceiros

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

Desinstalar Python

Passos

1. No **Painel de Controle** selecione **Programas > Programas e Recursos**.
2. Selecione Python na lista de programas.
3. Selecione **Desinstalar este programa**. Desinstale qualquer versão do Python, exceto a 3.12. Certifique-se de manter a versão 3.12 do Python.

Desinstalar o Microsoft Visual C++ 2013

Passos

1. No **Painel de Controle** selecione **Programas > Programas e Recursos**.
2. Selecione **Microsoft Visual C++ 2013** na lista de programas.
3. Selecione **Desinstalar este programa**.

Reiniciar o Unified Manager

Talvez seja necessário reiniciar o Unified Manager após fazer alterações na configuração.

Antes de começar

Você deve ter privilégios de administrador do Windows.

Passos

1. Efetue login no Windows usando a conta de administrador local padrão.
2. Pare os serviços do Unified Manager:

Do...	Pare os serviços na seguinte ordem...
Linha de comando	a. <code>sc stop ocie-au</code> b. <code>sc stop Oncommandsvc</code>

Do...	Pare os serviços na seguinte ordem...
Gerenciador de Serviços da Microsoft	a. Serviço de aquisição NetApp Active IQ (Ocie-au) b. Serviço de servidor de gerenciamento NetApp Active IQ (Oncommandsvc)

3. Inicie os serviços do Unified Manager:

Do...	Inicie os serviços na seguinte ordem...
Linha de comando	a. <code>sc start Oncommandsvc</code> b. <code>sc start ocie-au</code>
Gerenciador de Serviços da Microsoft	a. Serviço de servidor de gerenciamento NetApp Active IQ (Oncommandsvc) b. Serviço de aquisição NetApp Active IQ (Ocie-au)

Desinstalar o Unified Manager

Você pode desinstalar o Unified Manager usando o assistente de Programas e Recursos ou executando uma desinstalação autônoma na interface de linha de comando.

Antes de começar

- Você deve ter privilégios de 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 3306 do MySQL. 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:
 - Navegue até **Painel de Controle > Programas e Recursos**.
 - Selecione Active IQ Unified Manager e clique em **Desinstalar**.
- Se você desinstalar o Unified Manager pela linha de comando, execute estas etapas:
 - Efetue login na linha de comando do Windows usando privilégios de administrador.
 - Navegue até o diretório do 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 habilitado no servidor e você estiver conectado como

um usuário de domínio, será necessário usar o método de desinstalação por linha de comando.

O Unified Manager foi desinstalado do seu 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++ 2015 Redistributable, Python e 7zip
 - Dados do aplicativo MySQL gerados pelo Unified Manager
 - Logs de aplicativos e conteúdo do diretório de dados do aplicativo

Executar tarefas de configuração e administrativas

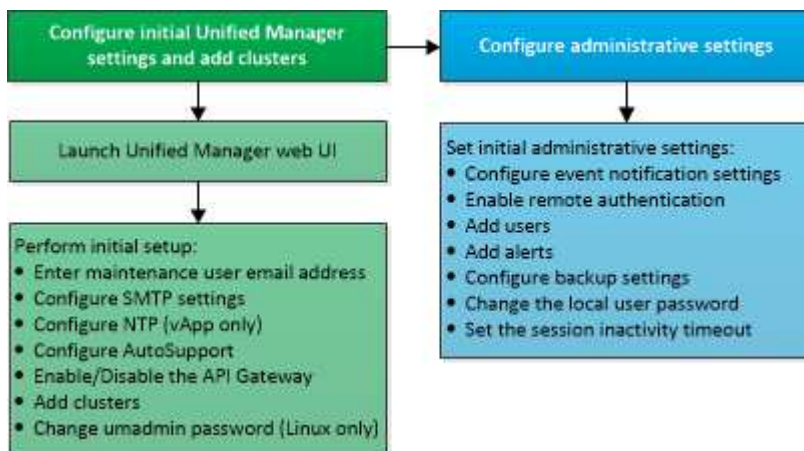
Configurar o Active IQ Unified Manager

Após instalar o Active IQ Unified Manager (antigo OnCommand Unified Manager), você deve concluir a configuração inicial (também chamada de assistente de primeira experiência) para acessar a interface da web. Em seguida, 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 sua instância do Unified Manager. Outros procedimentos são definições de configuração recomendadas que são úteis para configurar em sua nova instância ou que é bom saber antes de iniciar o monitoramento regular de seus sistemas ONTAP .

Visão geral da sequência de configuração

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



Acesse a interface da Web do Unified Manager

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

Antes de começar

- Se esta for a primeira vez que você acessa a interface da web, você deve efetuar login como usuário de manutenção (ou usuário umadmin para instalações Linux).
- Se você planeja permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o nome de domínio totalmente qualificado (FQDN) ou endereço IP, sua configuração de rede precisa 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 interface de usuário da Web do Unified Manager no seu navegador usando o URL exibido no final da instalação. O URL é o endereço IP ou nome de domínio totalmente qualificado (FQDN) do servidor do Unified Manager.

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

2. Efetue login na interface da Web do Unified Manager usando suas credenciais de usuário de manutenção.



Se você fizer três tentativas consecutivas sem sucesso de login na interface da web em uma hora, seu acesso ao sistema será bloqueado e você precisará entrar em contato com o administrador do sistema. Isso é aplicável somente a usuários locais.

Execute a configuração inicial da interface da Web do Unified Manager

Para usar o Unified Manager, você deve primeiro configurar as opções de instalação 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:

- Iniciou a interface de usuário da Web do Unified Manager usando o URL fornecido após a instalação
- Efetuiu login usando o nome de usuário e a senha de manutenção (usuário umadmin para instalações Linux) criados durante a instalação

A página de introdução do Active IQ Unified Manager aparece somente quando você acessa a interface da Web pela primeira vez. A página abaixo é de uma instalação no VMware.

≡

Active IQ Unified Manager

All ▾

Search All Storage Objects and Actions 🔍

Getting Started

1

2

3

4

5

EmailAutoSupportAPI GatewayAdd ONTAP ClustersFinish

Notifications

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

Maintenance User Email

Emailmgo@eng.netapp.com

SMTP Server

Host Name or IP Addressemail.eng.netapp.com

Port25

User Nameadmin

Password

☐ Use STARTTLS ⓘ ☐ Use SSL ⓘ

Continue

Se desejar alterar qualquer uma dessas opções posteriormente, você poderá selecionar sua escolha nas opções Gerais no painel de navegação esquerdo do Unified Manager. Observe que a configuração do NTP é somente para instalações do 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 SMTP adicionais, e o servidor NTP (somente instalações VMware). Em seguida, clique em **Continuar**.



Se você selecionou a opção **Usar STARTTLS** ou **Usar SSL**, uma página de certificado será exibida depois que você clicar no botão **Continuar**. Verifique os detalhes do certificado e aceite o certificado para continuar com as configurações iniciais da interface web.

2. Na página AutoSupport , clique em **Concordar e continuar** para habilitar o envio de mensagens de AutoSupport do Unified Manager para o NetAppActive IQ.

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

3. Em sistemas Red Hat, altere a senha do usuário `umadmin` da string padrão `admin` para uma string personalizada.
4. Na página Configurar API Gateway, selecione se deseja usar o recurso API Gateway que permite ao Unified Manager gerenciar os clusters ONTAP que você planeja monitorar usando APIs REST ONTAP . Em seguida, clique em **Continuar**.

Você pode habilitar ou desabilitar essa configuração mais tarde na interface da web em **Geral > Configurações de recursos > Gateway de API**. Para obter mais informações sobre as APIs, consulte "[Introdução às APIs REST do Active IQ Unified Manager](#)".

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

Esta etapa é opcional. Você pode adicionar clusters mais tarde na interface 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 é fechada e a página Painel do Unified Manager é exibida.

Adicionar clusters

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

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter as seguintes informações:
 - O Unified Manager oferece suporte a clusters ONTAP locais, ONTAP Select e 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 do cluster.

O endereço IP de gerenciamento de cluster deve ser o LIF de gerenciamento de cluster da máquina virtual de armazenamento 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

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

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

Certificado SSL (HTTPS): Este certificado é de propriedade do Unified Manager. Um certificado SSL

autoassinado padrão (HTTPS) é gerado com uma nova instalação do Unified Manager. A NetApp recomenda que você atualize para um certificado assinado por CA para maior 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 a regeneração do certificado SSL, consulte ["Gerando um certificado de segurança HTTPS"](#) .

Certificado EMS: Este certificado é de propriedade do Unified Manager. 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 habilitada 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 será habilitada.

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



- Você pode adicionar um cluster a partir da interface da web, e a autenticação baseada em certificado será ativada automaticamente.
- Você pode adicionar um cluster por meio do Unified Manager CLI; 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 interface do usuário do Unified Manager. Você pode ver ["Comandos CLI do Unified Manager suportados"](#) para adicionar um cluster usando o Unified Manager CLI.
- Se a autenticação baseada em certificado estiver habilitada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurar em outro servidor do Unified Manager onde o nome do host ou endereço IP for alterado, o monitoramento do cluster poderá falhar. Para evitar a falha, edite e salve os detalhes do cluster. Para obter mais informações sobre a edição de detalhes do cluster, consulte ["Editando clusters"](#) .

+

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 deverá 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 autoassinado ONTAP na interface de usuário do System Manager"](#) .

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

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

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de cluster**.
2. Na página Configuração do cluster, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar cluster, especifique os valores necessários, como o nome do host ou endereço IP do cluster, nome de usuário, senha e 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 a conclusão do próximo ciclo de monitoramento.

4. Clique em **Enviar**.
5. Na caixa de diálogo Autorizar Host, clique em **Exibir Certificado** para visualizar as informações do certificado sobre o cluster.
6. Clique em **Sim**.

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

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

Depois que todos os objetos de um novo cluster são descobertos, o Unified Manager começa a coletar dados históricos de desempenho dos 15 dias anteriores. Essas estatísticas são coletadas usando a funcionalidade de coleta de continuidade de dados. Este recurso fornece mais de duas semanas de informações de desempenho para um cluster imediatamente após ele 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 15 dias de dados de desempenho exige muita CPU, é recomendável escalonar 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 ausente.



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

Informações relacionadas

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

Configurar 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

Você deve ter a função de Administrador do Aplicativo.

Após implantar o Unified Manager e concluir a configuração inicial, você deve considerar configurar seu ambiente para acionar alertas e gerar e-mails de notificação ou interceptações 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, você deve configurar um servidor SMTP e fornecer um endereço de e-mail 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. "Habilitar autenticação remota".

Se você quiser que usuários remotos do LDAP ou do Active Directory acessem a instância do Unified Manager e recebam notificações de alerta, será necessário habilitar 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 usuários".

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 as notificações, configurar suas configurações de rede e configurar as opções SMTP e SNMP necessárias para seu ambiente, você poderá atribuir alertas.

Configurar as definições de notificação de eventos

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

Antes de começar

Você deve ter as seguintes informações:

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

Para especificar vários destinos de interceptação, separe cada host com uma vírgula. Nesse caso, todas as outras configurações SNMP, como versão e porta de interceptação de saída, devem ser as mesmas

para todos os hosts na lista.

Você deve ter a função de Administrador de Aplicativos 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 estiver preenchido com o endereço "ActiveQUnifiedManager@localhost.com", você deverá alterá-lo para um endereço de e-mail real e funcional para garantir que todas as notificações por 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 selecionou a opção **Usar STARTTLS** ou **Usar SSL**, uma página de certificado será exibida depois que você clicar no botão **Salvar**. 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 visualizar 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 visualizar um novo certificado.

Habilitar 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 de armazenamento e dados.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.



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

Você pode habilitar a autenticação remota usando o Open LDAP ou o Active Directory. Se a autenticação remota estiver desabilitada, os usuários remotos não poderão acessar o Unified Manager.

A autenticação remota é suportada por LDAP e LDAPS (LDAP seguro). O Unified Manager usa 389 como a porta padrão para comunicação não segura e 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...	Insira as seguintes informações...
Diretório ativo	• Nome do administrador do servidor de autenticação em um dos seguintes formatos: ◦ domainname\username ◦ username@domainname ◦ Bind Distinguished Name(usando a notação LDAP apropriada) • Senha do administrador • Nome distinto base (usando a notação LDAP apropriada)
Abra o LDAP	• Vincular nome distinto (na notação LDAP apropriada) • Vincular senha • Nome distinto base

Se a autenticação de um usuário do Active Directory demorar muito ou atingir o tempo limite, o servidor de autenticação provavelmente está demorando muito para responder. Desabilitar 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 Secure Sockets Layer (SSL).

4. **Opcional:** Adicione servidores de autenticação e teste a autenticação.

5. Clique em **Salvar**.

Desabilitar grupos aninhados da autenticação remota

Se você tiver a autenticação remota habilitada, poderá desabilitar a autenticação de grupo aninhada para que somente usuários individuais, e não membros do grupo, possam se autenticar remotamente no Unified Manager. Você pode desabilitar grupos aninhados quando quiser melhorar o tempo de resposta da autenticação do Active Directory.

Antes de começar

- Você deve ter a função de Administrador do Aplicativo.
- A desabilitação de grupos aninhados só é aplicável ao usar o Active Directory.

Desabilitar o suporte para grupos aninhados no Unified Manager pode reduzir o tempo de autenticação. Se o suporte a grupos aninhados estiver desabilitado 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 grupo aninhado**.
3. Clique em **Salvar**.

Configurar serviços de autenticação

Os serviços de autenticação permitem a autenticação de usuários remotos ou grupos remotos em um servidor de autenticação antes de fornecer a eles 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

- Você deve ter habilitado a autenticação remota.
- Você deve ter a função de Administrador do Aplicativo.

Passos

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

Se você selecionar...	Então faça isto...
Diretório ativo	a. Digite o nome e a senha do administrador. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for <code>ou@domain.com</code>, o nome distinto base será cn=ou,dc=domain,dc=com.
OpenLDAP	a. Digite o nome distinto e a senha de vinculação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for <code>ou@domain.com</code>, o nome distinto base será cn=ou,dc=domain,dc=com.

Se você selecionar...	Então faça isto...
Outros	a. Digite o nome distinto e a senha de vinculação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for <code>ou@domain.com</code>, o nome distinto base será cn=ou,dc=domain,dc=com. c. Especifique a versão do protocolo LDAP suportada pelo servidor de autenticação. d. Insira o nome do usuário, a associação ao grupo, o grupo de usuários e os atributos do membro.



Se quiser modificar o serviço de autenticação, você deverá excluir todos os servidores de autenticação existentes e, em seguida, adicionar novos servidores de autenticação.

3. Clique em **Salvar**.

Adicionar servidores de autenticação

Você pode adicionar servidores de autenticação e habilitar a autenticação remota no servidor de gerenciamento para que usuários remotos dentro do 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 seu serviço de autenticação para que o servidor de gerenciamento possa autenticar usuários ou grupos remotos no servidor de autenticação.
- Você deve ter a função de Administrador do Aplicativo.

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 do parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação estiver inacessível.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação Remota**.
2. Habilite ou desabilite a opção **Usar conexão segura**:

Se você quiser...	Então faça isto...
Habilite-o	a. Selecione a opção Usar conexão segura. b. Na área Servidores de autenticação, clique em Adicionar. c. Na caixa de diálogo Adicionar servidor de autenticação, insira o nome de autenticação ou endereço IP (IPv4 ou IPv6) do servidor. d. Na caixa de diálogo Autorizar Host, clique em Exibir Certificado. e. Na caixa de diálogo Exibir certificado, verifique as informações do certificado e clique em Fechar. f. Na caixa de diálogo Autorizar Host, clique em Sim.  Quando você habilita a opção Usar autenticação de conexão segura, o Unified Manager se comunica com o servidor de autenticação e exibe o certificado. O Unified Manager usa 636 como porta padrão para comunicação segura e a porta número 389 para comunicação não segura.
Desabilite-o	a. Desmarque a opção Usar conexão segura. b. Na área Servidores de autenticação, clique em Adicionar. 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. d. Clique em Adicionar.

O servidor de autenticação que você adicionou é exibido na área Servidores.

3. Execute um teste de autenticação para confirmar se você pode autenticar usuários no servidor de autenticação que você adicionou.

Teste a configuração dos servidores de autenticação

Você pode validar a configuração dos seus servidores de autenticação para garantir que o servidor de gerenciamento consiga se comunicar com eles. Você pode validar a configuração pesquisando um usuário remoto ou grupo remoto em seus servidores de autenticação e autenticando-os usando as configurações definidas.

Antes de começar

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

Se o serviço de autenticação estiver definido como Active 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 da autenticação.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação Remota**.
2. Clique em **Testar autenticação**.
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 **Testar**.

Se você estiver autenticando um grupo remoto, não deverá digitar a senha.

Adicionar alertas

Você pode configurar alertas para notificá-lo quando um evento específico for 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 as configurações de notificação, como o endereço de e-mail do usuário, o servidor SMTP e o host de interceptação SNMP para permitir que o servidor Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento for gerado.
- Você deve saber os recursos e eventos para os quais deseja acionar o alerta, além dos nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se quiser que um script seja executado com base no evento, você deve adicionar o script ao Unified Manager usando a página Scripts.
- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode criar um alerta diretamente na página Detalhes do evento após 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 sequência de texto no campo **Nome contém** para selecionar um grupo de recursos. Com base na sequência de texto especificada, a lista de recursos

disponíveis exibe apenas aqueles que correspondem à regra de filtro. A sequência de texto que você especificar diferencia maiúsculas de minúsculas.

Se um recurso estiver em conformidade com as regras de inclusão e exclusão especificadas, a regra de exclusão terá precedência sobre a regra de inclusão, 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 o qual você deseja acionar um alerta.



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

6. Clique em **Ações** e selecione os usuários que deseja notificar, escolha a frequência de notificação, escolha se uma armadilha SNMP será enviada ao receptor da armadilha 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 aparecerá em branco porque o endereço de e-mail modificado não estará mais mapeado para o usuário selecionado anteriormente. Além disso, se você modificar 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 por meio de traps SNMP.

7. Clique em **Salvar**.

Exemplo de adição de um alerta

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

- Nome do alerta: HealthTest
- Recursos: inclui todos os volumes cujo nome contém "abc" e exclui todos os volumes cujo nome contém "xyz"
- Eventos: inclui todos os eventos críticos de saúde
- Ações: inclui "sample@domain.com", um script "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 **HealthTest** 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'] +** da área Recursos Disponíveis e mova-o para a área Recursos Selecionados.
 - c. Clique em **Excluir** e insira **xyz** no campo **Nome contém** e depois clique em **Adicionar**.
3. Clique em **Eventos** e selecione **Crítico** no campo Gravidade do Evento.
4. Selecione **Todos os Eventos Críticos** na área Eventos Correspondentes e mova-os para a área Eventos Selecionados.
5. Clique em **Ações** e insira **sample@domain.com** no campo Alertar estes usuários.

6. Selecione **Lembrar a cada 15 minutos** para notificar o usuário a cada 15 minutos.

Você pode configurar um alerta para enviar notificações repetidamente aos destinatários por um período específico. Você deve determinar o horário a partir do qual a notificação de evento estará ativa para o alerta.

7. No menu Selecionar script para executar, selecione o script **Teste**.

8. Clique em **Salvar**.

Alterar a senha do usuário local

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

Antes de começar

Você deve estar logado como usuário local.

As senhas do usuário de manutenção e dos usuários remotos não podem ser alteradas usando estas etapas. Para alterar a senha de um usuário remoto, entre em contato com o administrador de senhas. Para alterar a senha do usuário de manutenção, consulte "[Usando o console de manutenção](#)".

Passos

1. Efetue login no Unified Manager.
2. Na barra de menu superior, clique no ícone do usuário e depois clique em **Alterar senha**.

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

3. Na caixa de diálogo Alterar senha, digite 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 do tempo limite de inatividade do Unified Manager para que a sessão seja encerrada automaticamente após um determinado período de inatividade. Por padrão, o tempo limite é definido como 4.320 minutos (72 horas).

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Esta configuração afeta todas as sessões de usuários conectados.



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

Passos

1. No painel de navegação esquerdo, clique em **Geral > Configurações de recursos**.
2. Na página **Configurações de recursos**, especifique o tempo limite de inatividade escolhendo uma das

seguintes opções:

Se você quiser...	Então faça isto...
Não defina nenhum tempo limite para que a sessão nunca seja fechada automaticamente	No painel Tempo limite de inatividade , mova o botão deslizante para a esquerda (desligado) e clique em Aplicar .
Defina um número específico de minutos como valor de tempo limite	No painel Tempo limite de inatividade , mova o botão deslizante para a direita (ligado), especifique o valor do tempo limite de inatividade em minutos e clique em Aplicar .

Defina o tempo limite da sessão por meio da CLI

Você pode definir um valor máximo de tempo limite de sessão para o Unified Manager usando a CLI para que a sessão seja encerrada automaticamente após um determinado período de tempo. Por padrão, o tempo limite da sessão é definido para o valor máximo, que é 4.320 minutos (72 horas). Isso significa que sua sessão termina automaticamente após 72 horas, mesmo que você esteja conectado e usando ativamente o Unified Manager.

Sobre esta tarefa

Você deve ter a função de Administrador do Aplicativo.

A configuração de tempo limite de sessão afeta todas as sessões de usuários conectados.

Passos

1. Efetue login no Unified Manager CLI inserindo o um `cli login` comando. Use um nome de usuário e senha válidos para autenticação.
2. Entre no um `option set max.session.timeout.value=<in mins>` comando para modificar o valor do tempo limite da sessão.

Alterar o nome do host do Unified Manager

Em algum momento, você pode querer alterar o nome do host do sistema no qual 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.

Alterar o nome do host do appliance 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, também deverá gerar novamente o certificado HTTPS.

Antes de começar

Você deve estar conectado ao Unified Manager como usuário de manutenção ou ter a função de 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 interface da Web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, você teria designado um nome para o host da rede. Se você configurou a rede usando DHCP, o nome do host deve ser obtido do DNS. Se o DHCP ou o DNS não estiver configurado corretamente, o nome do host “Unified Manager” será automaticamente atribuído e associado ao certificado de segurança.

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

Se você acessar a interface da Web usando o endereço IP do servidor em vez do nome do host, não precisará gerar um novo certificado se alterar o nome do host. No entanto, a melhor prática é 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, deverá atualizá-lo manualmente 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 reiniciada.

Passos

1. Gerar um certificado de segurança HTTPS

Se quiser usar o novo nome de host para acessar a interface de usuário da Web do Unified Manager, você deverá gerar novamente 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.

Gerar 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

Você deve ter a função de Administrador do Aplicativo.

Pode haver vários motivos para regenerar o certificado, como se você desejasse ter valores melhores para Nome Distinto (DN), se quisesse um tamanho de chave maior, um período de expiração mais longo ou se o certificado atual tivesse expirado.

Se você não tiver acesso à interface da Web do Unified Manager, poderá gerar novamente 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 o `Reset Server Certificate` opção do console de manutenção, então um novo certificado HTTPS é criado e é 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 **Regenerar certificado HTTPS**.

A caixa de diálogo Regenerar certificado HTTPS é exibida.

3. Selecione uma das seguintes opções dependendo de como você deseja gerar o certificado:

Se você quiser...	Faça isso...
Regenerar o certificado com os valores atuais	Clique na opção Regenerar usando atributos de certificado atuais .

Se você quiser...	Faça isso...
Gerar o certificado usando valores diferentes	Clique na opção Atualizar os atributos atuais do certificado. 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 E-MAIL, EMPRESA, DEPARTAMENTO, Cidade, Estado e País, se quiser que esses valores sejam preenchidos no certificado. Você também pode selecionar entre o TAMANHO DA CHAVE disponível (o algoritmo da chave é “RSA”). e o PERÍODO DE VALIDADE.  • Os valores permitidos para o tamanho da chave são 2048 , 3072 e 4096 . • Os períodos de validade são de no mínimo 1 dia e no máximo 36.500 dias. Embora seja permitido um período de validade de 36.500 dias, é recomendável usar um período de validade de no máximo 397 dias ou 13 meses. Porque se você selecionar um período de validade de mais de 397 dias e planejar exportar um CSR para este certificado e obtê-lo assinado por uma CA conhecida, a validade do certificado assinado devolvido a você pela CA será reduzida para 397 dias. • Você pode selecionar a caixa de seleção “Excluir informações de identificação local (por exemplo, host local)” se quiser remover as informações de identificação local do campo Nomes alternativos no certificado. Quando esta caixa de seleção estiver marcada, somente o que você inserir no campo será usado no campo Nomes Alternativos. Se deixado em branco, o certificado resultante não terá nenhum campo Nomes Alternativos.

4. Clique em **Sim** 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.

Reinicie a máquina virtual do Unified Manager

Você pode reiniciar a máquina virtual no console de manutenção do Unified Manager. Você deve reiniciar após 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 **Reiniciar Convidado**. Consulte a documentação do VMware para obter mais informações.

Passos

1. Acesse o console de manutenção.
2. Selecione **Configuração do sistema > Reinicializar máquina virtual**.

Alterar o nome do 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 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 ao listar suas máquinas Linux.

Antes de começar

Você deve ter acesso de usuário root 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 interface da Web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, você teria designado um nome para o host da rede. Se você configurou a rede usando DHCP, o nome do host deve ser obtido do servidor DNS.

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

Se você acessar a interface da Web usando o endereço IP do servidor em vez do nome do host, não precisará gerar um novo certificado se alterar o nome do host. No entanto, a melhor prática é atualizar o certificado para que o nome do host no certificado corresponda ao nome do host real. O novo certificado não entrará em vigor até que a máquina Linux seja reiniciada.

Se você alterar o nome do host no Unified Manager, deverá atualizá-lo manualmente no OnCommand Workflow Automation (WFA). O nome do host não é atualizado automaticamente no WFA.

Passos

1. Efetue login como usuário root no sistema Unified Manager que você deseja modificar.

2. Pare o software Unified Manager e o software MySQL associado inserindo o seguinte comando:

```
systemctl stop ocieau ocie mysqld
```

3. Alterar o nome do host usando o Linux `hostnamectl` comando:

```
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. Após o serviço ser reiniciado, verifique se o novo nome do host consegue 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 do host original.

7. Após concluir e verificar a alteração do nome do host, reinicie o Unified Manager digitando o seguinte comando:

```
systemctl start mysqld ocie ocieau
```

Habilitar e desabilitar o gerenciamento de armazenamento baseado em políticas

A partir do Unified Manager 9.7, você pode provisionar cargas de trabalho de armazenamento (volumes e LUNs) em seus clusters ONTAP e gerenciar essas cargas de trabalho com base nos níveis de serviço de desempenho atribuídos. Essa funcionalidade é semelhante à criação de cargas de trabalho no ONTAP System Manager e à anexação de políticas de QoS, mas quando aplicada usando o Unified Manager, você pode provisionar e gerenciar cargas de trabalho em todos os clusters que sua instância do Unified Manager está monitorando.

Você deve ter a função de Administrador do Aplicativo.

Esta opção é habilitada por padrão, mas você pode desabilitá-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 usuário:

Novo conteúdo	Localização
Uma página para provisionar novas cargas de trabalho	Disponível em Tarefas comuns > Provisionamento
Uma página para criar políticas de nível de serviço de desempenho	Disponível em Configurações > Políticas > Níveis de serviço de desempenho
Uma página para criar políticas de eficiência de armazenamento de desempenho	Disponível em Configurações > Políticas > Eficiência de armazenamento
Painéis que descrevem seu desempenho de carga de trabalho atual e IOPS de carga de trabalho	Disponível no Pannel

Consulte a ajuda on-line do produto para obter mais informações sobre essas páginas e essa funcionalidade.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Configurações de recursos**.
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 isto...
Desabilitar o gerenciamento de armazenamento baseado em políticas	No painel Gerenciamento de armazenamento baseado em políticas , mova o botão deslizante para a esquerda.
Habilitar gerenciamento de armazenamento baseado em políticas	No painel Gerenciamento de armazenamento baseado em políticas , mova o botão deslizante para a direita.

Configurar 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 por meio do console de manutenção.

Para obter informações sobre as etapas de configuração, consulte "[Gerenciando operações de backup e restauração](#)".

Gerenciar configurações de recursos

A página Configurações de recursos permite que você habilite e desabilite recursos específicos no Active IQ Unified Manager. Isso inclui criar e gerenciar objetos de armazenamento com base em políticas, habilitar o API Gateway e o Login Banner, carregar scripts para gerenciar alertas, tempo limite de uma sessão da interface do usuário da Web com base no tempo de inatividade e desabilitar o recebimento de

eventos da plataforma Active IQ .



A página Configurações de recursos está disponível somente para usuários com função de Administrador do aplicativo.

Para obter informações sobre o upload de scripts, consulte "[Habilitando e desabilitando o upload de scripts](#)".

Habilitar gerenciamento de armazenamento baseado em políticas

A opção **Gerenciamento de armazenamento baseado em políticas** permite o gerenciamento de armazenamento com base em objetivos de nível de serviço (SLOs). Esta opção é habilitada por padrão.

Ao ativar esse recurso, você pode provisionar cargas de trabalho de armazenamento nos clusters ONTAP adicionados à sua instância do Active IQ Unified Manager e gerenciar essas cargas de trabalho com base nos Níveis de Serviço de Desempenho e Políticas de Eficiência de Armazenamento atribuídos.

Você pode optar por ativar ou desativar esse recurso em **Geral > Configurações de recursos > Gerenciamento de armazenamento baseado em políticas**. Ao ativar este recurso, as seguintes páginas estarão disponíveis para operação e monitoramento:

- Provisionamento (provisionamento de carga de trabalho de armazenamento)
- **Políticas > Níveis de Serviço de Desempenho**
- **Políticas > Eficiência de Armazenamento**
- Coluna Cargas de trabalho gerenciadas por nível de serviço de desempenho na página Configuração de clusters
- Painel de desempenho da carga de trabalho no **Painel**

Você pode usar as telas para criar Níveis de Serviço de Desempenho e Políticas de Eficiência de Armazenamento, além de provisionar cargas de trabalho de armazenamento. Você também pode monitorar as cargas de trabalho de armazenamento que estão em conformidade com os Níveis de Serviço de Desempenho atribuídos, bem como as que não estão em conformidade. O painel Desempenho da carga de trabalho e IOPS da carga de trabalho também permite que você avalie a capacidade e o desempenho (IOPS) total, disponível e usado dos clusters em seu data center com base nas cargas de trabalho de armazenamento provisionadas neles.

Após ativar esse recurso, você pode executar as APIs REST do Unified Manager para executar algumas dessas funções em **Barra de menus > Botão Ajuda > Documentação da API > categoria provedor de armazenamento**. Como alternativa, você pode inserir o nome do host ou endereço IP e a URL para acessar a página da API REST no formato `https://<nome do host>/docs/api/`

Para obter mais informações sobre as APIs, consulte "[Introdução às APIs REST do Active IQ Unified Manager](#)".

Habilitar 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 precisar fazer login neles individualmente.

Você pode habilitar esse recurso nas páginas de configuração que aparecem quando você faz login pela

primeira vez no Unified Manager. Como alternativa, você pode habilitar ou desabilitar esse recurso em **Geral > Configurações de recursos > Gateway de 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 usando as APIs REST do Unified Manager. No entanto, se você tiver um requisito comercial específico de acesso às APIs do ONTAP para gerenciar recursos específicos que não são expostos ao Unified Manager, você pode habilitar o recurso API Gateway e executar as APIs do ONTAP . O gateway atua como um proxy para encapsular as solicitações de API, mantendo o cabeçalho e o corpo das solicitações no mesmo formato das APIs ONTAP . Você pode usar suas credenciais do Unified Manager e executar as APIs específicas para acessar e gerenciar os clusters ONTAP sem passar credenciais de cluster individuais. O Unified Manager funciona como um único ponto de gerenciamento para executar as APIs nos clusters 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.

Após habilitar esse recurso, você pode executar as APIs REST do Unified Manager em **Barra de Menu > Botão Ajuda > Documentação da API > categoria gateway**. Como alternativa, você pode inserir o nome do host ou endereço IP e a URL para acessar a página da API REST no formato <https://<hostname>/docs/api/>

Para obter mais informações sobre as APIs, consulte "[Introdução às APIs REST do Active IQ Unified Manager](#)".

Especificar tempo limite de inatividade

Você pode especificar o valor do tempo limite de inatividade para o Active IQ Unified Manager. Após um período de inatividade especificado, o aplicativo será desconectado automaticamente. Esta opção é habilitada por padrão.

Você pode desativar esse recurso ou modificar o tempo em **Geral > Configurações de recursos > Tempo limite de inatividade**. Depois de ativar esse recurso, você deve especificar o limite de tempo de inatividade (em minutos) no campo **SAIR APÓS**, após o qual o sistema efetuará logout automaticamente. O valor padrão é 4320 minutos (72 horas).



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

Habilitar eventos do portal Active IQ

Você pode especificar se deseja habilitar ou desabilitar eventos do portal Active IQ . Esta configuração permite que o portal Active IQ descubra e exiba eventos adicionais sobre configuração do sistema, cabeamento e assim por diante. Esta opção é habilitada por padrão.

Ao habilitar esse recurso, o Active IQ Unified Manager exibe eventos descobertos pelo portal Active IQ . Esses eventos são criados executando um conjunto de regras em mensagens do AutoSupport geradas 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.

Você pode escolher ativar ou desativar esse recurso em **Geral > Configurações de recursos > Eventos Active IQ ***. Em sites sem acesso à rede externa, você deve carregar as regras manualmente em

*Gerenciamento de armazenamento > Configuração de evento > Carregar regras.

Este recurso é habilitado por padrão. Desabilitar esse recurso impede que os eventos do Active IQ sejam descobertos ou exibidos no Unified Manager. Quando desabilitado, habilitar esse recurso permite que o Unified Manager receba os eventos do Active IQ em um cluster em um horário predefinido de 00:15 para o fuso horário desse cluster.

Habilitar e desabilitar configurações de segurança para conformidade

Ao usar o botão **Personalizar** no painel **Painel de Segurança** da página Configurações de Recursos, você pode habilitar ou desabilitar os parâmetros de segurança para monitoramento de conformidade no Unified Manager.

As configurações habilitadas ou desabilitadas nesta página controlam o status geral de conformidade dos clusters e VMs de armazenamento no Unified Manager. Com base nas seleções, as colunas correspondentes ficam visíveis na exibição **Segurança: Todos os clusters** da página de inventário de clusters e na exibição **Segurança: Todas as VMs de armazenamento** da página de inventário de VMs de armazenamento.



Somente usuários com função de administrador podem editar essas configurações.

Os critérios de segurança para seus clusters ONTAP , VMs de armazenamento e volumes são avaliados em relação às recomendações definidas no "[Guia de reforço de segurança para NetApp ONTAP 9](#)". O painel Segurança no painel e a página Segurança exibem o status de conformidade de segurança padrão dos seus clusters, VMs de armazenamento e volumes. Eventos de segurança também são gerados e ações de gerenciamento são habilitadas para clusters e VMs de armazenamento que têm violações de segurança.

Personalizar configurações de segurança

Para personalizar as configurações de monitoramento de conformidade aplicáveis ao seu ambiente ONTAP , siga estas etapas:

Passos

1. Clique em **Geral > Configurações de recursos > Painel de segurança > Personalizar**. O pop-up **Personalizar configurações do painel de segurança** é exibido.



Os parâmetros de conformidade de segurança que você habilita ou desabilita podem afetar diretamente as exibições de segurança padrão, relatórios e relatórios agendados nas telas Clusters e VMs de armazenamento. Se você tiver carregado um relatório do Excel dessas telas antes de modificar os parâmetros de segurança, os relatórios do Excel baixados podem estar com defeito.

2. Para habilitar ou desabilitar as configurações personalizadas para seus clusters ONTAP , selecione a configuração geral necessária em **Cluster**. Para obter informações sobre as opções de personalização da conformidade do cluster, consulte "[Categorias de conformidade do cluster](#)".
3. Para habilitar ou desabilitar as configurações personalizadas para suas VMs de armazenamento, selecione a configuração geral necessária em **VM de armazenamento**. Para obter informações sobre as opções de personalização da conformidade da VM de armazenamento, consulte "[Categorias de conformidade de VM de armazenamento](#)".

Personalize as configurações de AutoSupport e autenticação

Na seção * Configurações do AutoSupport *, você pode especificar se o transporte HTTPS deve ser usado

para enviar mensagens do AutoSupport do ONTAP.

Na seção **Configurações de autenticação**, você pode habilitar alertas do Unified Manager para serem gerados para o usuário administrador padrão do ONTAP .

Habilitar e desabilitar upload de scripts

A capacidade de carregar scripts no Unified Manager e executá-los é habilitada por padrão. Se sua organização não quiser permitir essa atividade por motivos de segurança, você pode desabilitar essa funcionalidade.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Configurações de recursos**.
2. Na página **Configurações de recursos**, desative ou ative o script escolhendo uma das seguintes opções:

Se você quiser...	Então faça isto...
Desabilitar scripts	No painel Script Upload , mova o botão deslizante para a esquerda.
Habilitar scripts	No painel Script Upload , mova o botão deslizante para a direita.

Adicionar banner de login

Adicionar um banner de login permite que sua organização exiba qualquer informação, como quem tem permissão para acessar o sistema e os termos e condições de uso durante o login e o logout.

Qualquer usuário, como operadores de armazenamento ou administradores, pode visualizar este pop-up de banner de login durante o login, logout e tempo limite da sessão.

Use o console de manutenção

Você pode usar o console de manutenção para configurar 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 do seu sistema 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 quaisquer problemas com seu dispositivo virtual, especialmente se a interface da Web do Unified Manager não estiver disponível
- Atualize para versões mais recentes do Unified Manager
- Gerar pacotes de suporte para enviar ao suporte técnico
- Configurar as configurações de rede
- Alterar a senha do usuário de manutenção
- Conecte-se a um provedor de dados externo para enviar estatísticas de desempenho
- Alterar a coleta interna de dados de desempenho
- Restaure o banco de dados do Unified Manager e as definições de configuração de uma versão de backup anterior.

O que o usuário de manutenção faz

O usuário de manutenção é criado durante a instalação do Unified Manager em um sistema Red Hat Enterprise Linux. O nome do usuário de manutenção é o usuário “umadmin”. O usuário de manutenção tem a função de Administrador do Aplicativo na interface do usuário da Web e pode criar usuários subsequentes e atribuir funções a eles.

O usuário de manutenção, ou usuário umadmin, também pode acessar o console de manutenção do Unified Manager.

Capacidades de diagnóstico do usuário

O objetivo do acesso de diagnóstico é permitir que o suporte técnico auxilie você na solução de problemas, e você só deve usá-lo quando instruído pelo suporte técnico.

O usuário de diagnóstico pode executar comandos no nível do sistema operacional quando instruído pelo suporte técnico, para fins de solução de problemas.

Acesse o console de manutenção

Se a interface do usuário do Unified Manager não estiver em operação ou se você precisar executar funções que não estão disponíveis na interface do usuário, você poderá acessar o console de manutenção para gerenciar seu sistema Unified Manager.

Antes de começar

Você deve ter instalado e configurado o Unified Manager.

Após 15 minutos de inatividade, o console de manutenção desconecta você.



Quando instalado no VMware, se você já tiver efetuado login como usuário de manutenção por meio do console do VMware, não será possível efetuar login simultaneamente usando o Secure Shell.

Etapa

1. Siga estas etapas para acessar o console de manutenção:

Neste sistema operacional...	Siga estes passos...
VMware	a. Usando o Secure Shell, conecte-se ao endereço IP ou ao nome de domínio totalmente qualificado do dispositivo virtual do Unified Manager. b. Efetue login no console de manutenção usando seu nome de usuário e senha de manutenção.
Linux	a. Usando o Secure Shell, conecte-se ao endereço IP ou ao nome de domínio totalmente qualificado do sistema Unified Manager. b. Efetue login no sistema com o nome de usuário de manutenção (umadmin) e a senha. c. Digite o comando <code>maintenance_console</code> e pressione Enter.
Windows	a. Efetue login no sistema Unified Manager com credenciais de administrador. b. Inicie o PowerShell como administrador do Windows. c. Digite o comando <code>maintenance_console</code> e pressione Enter.

O menu do console de manutenção do Unified Manager é exibido.

Acesse o console de manutenção usando o console da VM do vSphere

Se a interface do usuário do Unified Manager não estiver em operação ou se você precisar executar funções que não estão 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 estar ligado para acessar o console de manutenção.

Passos

1. No vSphere Client, localize o dispositivo virtual Unified Manager.
2. Clique na aba **Console**.
3. Clique dentro da janela do console para efetuar login.
4. Efetue login no console de manutenção usando seu nome de usuário e senha.

Após 15 minutos de inatividade, o console de manutenção desconecta você.

Menus do console de manutenção

O console de manutenção consiste em diferentes menus que permitem manter e gerenciar recursos especiais e definições de configuração 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. Redefinir certificado do servidor
 - c. Provedor de dados externo
 - d. Restauração de backup
 - e. Configuração do intervalo de pesquisa de desempenho
 - f. Desativar autenticação SAML
 - g. Exibir/Alterar Portas do Aplicativo
 - h. Configuração do log de depuração
 - i. Controle o acesso à porta 3306 do MySQL
 - j. Saída

Selecione o número na lista para acessar a opção de menu específica. Por exemplo, para backup e restauração, selecione 4.

Menu de configuração de rede

O menu Configuração de rede permite que você gerencie as configurações de rede. Você deve usar este menu quando a interface de usuário do Unified Manager não estiver disponível.



Este menu não estará disponível se o Unified Manager estiver instalado no Red Hat Enterprise Linux ou no Microsoft Windows.

As seguintes opções de menu estão disponíveis.

• Exibir configurações de endereço IP

Exibe as configurações de rede atuais do dispositivo virtual, incluindo endereço IP, rede, endereço de transmissão, máscara de rede, gateway e servidores DNS.

• Alterar configurações de endereço IP

Permite que você altere qualquer configuração de rede do dispositivo virtual, incluindo endereço IP, máscara de rede, gateway ou servidores DNS. Se você alternar suas configurações de rede de DHCP para rede estática usando o console de manutenção, não poderá editar o nome do host. Você deve

selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **Exibir configurações de pesquisa de nome de domínio**

Exibe a lista de pesquisa de nomes de domínio usada para resolver nomes de host.

- **Alterar configurações de pesquisa de nome de domínio**

Permite que você altere os nomes de domínio que deseja pesquisar ao resolver nomes de host. Você deve selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **Exibir rotas estáticas**

Exibe as rotas de rede estáticas atuais.

- **Alterar rotas estáticas**

Permite adicionar ou excluir rotas de rede estáticas. Você deve selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **Adicionar Rota**

Permite adicionar uma rota estática.

- **Excluir Rota**

Permite que você exclua uma rota estática.

- **Voltar**

Leva você de volta ao **Menu Principal**.

- **Saída**

Sai do console de manutenção.

- **Desabilitar interface de rede**

Desabilita todas as interfaces de rede disponíveis. Se apenas uma interface de rede estiver disponível, você não poderá desativá-la. Você deve selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **Habilitar interface de rede**

Habilita interfaces de rede disponíveis. Você deve selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **Confirmar alterações**

Aplica quaisquer alterações feitas nas configurações de rede do dispositivo virtual. Você deve selecionar esta opção para aplicar quaisquer alterações feitas, ou as alterações não ocorrerão.

- **Fazer ping em um host**

Faz ping em um host de destino para confirmar alterações de endereço IP ou configurações de DNS.

- **Restaurar para as configurações padrão**

Redefine todas as configurações para os padrões de fábrica. Você deve selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **Voltar**

Leva você de volta ao **Menu Principal**.

- **Saída**

Sai do console de manutenção.

Menu de configuração do sistema

O menu Configuração do Sistema permite que você gerencie seu dispositivo virtual fornecendo várias opções, como visualizar o status do servidor e reinicializar e desligar a máquina virtual.



Quando o Unified Manager é instalado em um sistema Linux ou Microsoft Windows, somente a opção “Restaurar de um backup do Unified Manager” está disponível neste menu.

As seguintes opções de menu estão disponíveis:

- **Exibir status do servidor**

Exibe o status atual do servidor. As opções de status incluem Em execução e Não em execução.

Se o servidor não estiver em execução, talvez seja necessário entrar em contato com o suporte técnico.

- **Reinicializar máquina virtual**

Reinicia a máquina virtual, interrompendo todos os serviços. Após a reinicialização, a máquina virtual e os serviços são reiniciados.

- **Desligar a máquina virtual**

Desliga a máquina virtual, interrompendo todos os serviços.

Você pode selecionar esta opção somente no console da máquina virtual.

- **Alterar senha do usuário <usuário conectado>**

Altera a senha do usuário que está conectado no momento, que só pode ser o usuário de manutenção.

- **Aumentar o tamanho do disco de dados**

Aumenta o tamanho do disco de dados (disco 3) na máquina virtual.

- **Aumentar o tamanho do disco de swap**

Aumenta o tamanho do disco de swap (disco 2) na máquina virtual.

- **Alterar fuso horário**

Altera o fuso horário para sua localização.

- **Alterar servidor NTP**

Altera as configurações do servidor NTP, como endereço IP ou nome de domínio totalmente qualificado (FQDN).

- **Alterar serviço NTP**

Alterna entre o `ntp` e `systemd-timesyncd` serviços.

- **Restaurar de um backup do Unified Manager**

Restaura o banco de dados e as definições de configuração do Unified Manager de uma versão de backup anterior.

- **Redefinir certificado do servidor**

Redefine o certificado de segurança do servidor.

- **Alterar nome do host**

Altera o nome do host no qual o dispositivo virtual está instalado.

- **Voltar**

Sai do menu Configuração do Sistema e retorna ao Menu Principal.

- **Saída**

Sai do menu do console de manutenção.

Menu de Suporte e Diagnóstico

O menu Suporte e Diagnóstico permite que você gere um pacote de suporte que pode ser enviado ao suporte técnico para obter assistência na solução de problemas.

As seguintes opções de menu estão disponíveis:

- **Gerar Pacote de Suporte de Luz**

Permite que você produza um pacote de suporte leve que contém apenas 30 dias de logs e registros de banco de dados de configuração — ele exclui dados de desempenho, arquivos de gravação de aquisição e despejo de heap do servidor.

- **Gerar Pacote de Suporte**

Permite que você crie um pacote de suporte completo (arquivo 7-Zip) contendo informações de diagnóstico no diretório inicial do usuário de diagnóstico. Se o seu sistema estiver conectado à Internet, você também poderá 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 Unified Manager, dados detalhados sobre os componentes internos do servidor do Unified Manager e logs de nível detalhado normalmente não incluídos em mensagens do AutoSupport ou no pacote de suporte leve.

Opções adicionais de menu

As seguintes opções de menu permitem que você execute várias tarefas administrativas no servidor do Unified Manager.

As seguintes opções de menu estão disponíveis:

- **Redefinir certificado do servidor**

Regenera o certificado do servidor HTTPS.

Você pode regenerar o certificado do servidor na GUI do Unified Manager clicando em **Geral > Certificados HTTPS > Regenerar certificado HTTPS**.

- **Desabilitar 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. Esta opção de console normalmente é usada quando um problema com o servidor IdP ou a configuração SAML impede que os usuários acessem a GUI do Unified Manager.

- **Provedor 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 a um servidor externo para que especialistas em desempenho de armazenamento possam mapear as métricas de desempenho usando software de terceiros. As seguintes opções são exibidas:

- **Exibir configuração do servidor** — Exibe as configurações atuais de conexão e configuração de 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.

Após a conexão ser excluída, o Unified Manager perde a conexão com o servidor externo.

- **Restauração de backup**

Para obter informações, consulte os tópicos em "[Gerenciando operações de backup e restauração](#)".

- **Configuração do intervalo de pesquisa de desempenho**

Fornece uma opção para configurar a frequência com que o Unified Manager coleta dados estatísticos de desempenho de clusters. O intervalo de coleta padrão é de 5 minutos.

Você pode alterar esse intervalo para 10 ou 15 minutos se perceber que as coletas de grandes clusters não estão sendo concluídas no prazo.

- **Ver/Alterar Portas de Aplicativos**

Fornece uma opção para alterar as portas padrão que o Unified Manager usa para os protocolos HTTP e HTTPS, se necessário para segurança. As portas padrão são 80 para HTTP e 443 para HTTPS.

- **Controle o acesso à porta 3306 do MySQL**

Controla o acesso do host à porta padrão do MySQL 3306. Por motivos de segurança, o acesso por essa porta é restrito apenas ao host local durante uma nova instalação do Unified Manager em sistemas Linux, Windows e VMware vSphere. Esta opção permite que você alterne a visibilidade desta porta entre o host local e os hosts remotos, ou seja, se ela estiver habilitada somente para o host local no seu ambiente, você também poderá disponibilizar esta porta para hosts remotos. Como alternativa, quando habilitado para todos os hosts, você pode restringir o acesso desta porta somente ao host local. Se o acesso foi habilitado em hosts remotos anteriormente, a configuração será mantida em um cenário de atualização. Você deve verificar as configurações de firewall em sistemas Windows depois de alternar a visibilidade da porta e desabilitar as configurações de firewall se as configurações estiverem definidas para restringir o acesso à porta 3306 do MySQL.

- **Saída**

Sai do menu do console de manutenção.

Alterar a senha do usuário 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 interface da web do Unified Manager, clique em **Esqueceu a senha**.

É exibida uma página solicitando o nome do usuário cuja senha você deseja redefinir.

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 **redefinir senha** no e-mail e defina a nova senha.
4. Retorne à interface da Web e faça login no Unified Manager usando a nova senha.

Alterar a senha do 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.

Antes de começar

- O Unified Manager deve ser instalado em um sistema Red Hat Enterprise Linux Linux.
- Você deve ter as credenciais de usuário root para o sistema Linux no qual o Unified Manager está instalado.

Passos

1. Efetue login como usuário root no sistema Linux no qual o Unified Manager está sendo executado.
2. Alterar a senha do 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 os protocolos HTTP e HTTPS

As portas padrão que o Unified Manager usa para os protocolos HTTP e HTTPS podem ser alteradas após a instalação, se necessário por questões de segurança. As portas padrão são 80 para HTTP e 443 para HTTPS.

Antes de começar

Você deve ter um ID de usuário e uma senha autorizados para efetuar 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 seu navegador antes de atribuir um novo número de porta para tráfego HTTP e HTTPS. Selecionar uma porta insegura pode tornar o sistema inacessível, o que exigirá que você entre em contato com o suporte ao cliente para obter uma resolução.

A instância do Unified Manager é reiniciada automaticamente depois que você altera a porta, portanto, certifique-se de que este seja um bom momento para desligar o sistema por um curto período.

1. Efetue login usando SSH como 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 rotulada **Exibir/Alterar portas de 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 perguntado se deseja alterar as portas e reiniciar o Unified Manager agora.

5. Digite **y** para alterar as portas e reiniciar o Unified Manager.
6. Saia do console de manutenção.

Após essa alteração, os usuários devem incluir o novo número de porta na URL para acessar a interface de usuário da Web do Unified Manager, 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).

Adicionar 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 do vSphere, selecione **Configuração do sistema > Reinicializar sistema operacional**.

Após a reinicialização, o console de manutenção pode detectar a interface de rede recém-adicionada.

2. Acesse o console 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 habilitar a interface de rede.
6. Digite as configurações de rede.

Você será solicitado a inserir as configurações de rede se estiver usando uma interface estática ou se o DHCP não for detectado.

Após inserir as configurações de rede, você retornará automaticamente ao menu **Configuração de rede**.

7. Selecione **Confirmar alterações**.

Você deve confirmar as alterações para adicionar a interface de rede.

Adicionar espaço em disco ao diretório do banco de dados do Unified Manager

O diretório de 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 dos clusters depois que o diretório atinge 95% da capacidade.

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.

Adicionar espaço ao diretório de dados do host Linux

Se você alocou espaço em disco insuficiente para o `/opt/netapp/data` diretório para oferecer suporte ao Unified Manager quando você configurou originalmente o host Linux e depois instalou o Unified Manager, você pode adicionar espaço em disco após a instalação aumentando o espaço em disco no `/opt/netapp/data` diretório.

Antes de começar

Você deve ter acesso de usuário root 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. Efetue 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 atual /opt/netapp/data diretório.
4. Copie o conteúdo e a configuração de privilégios do existente /opt/netapp/data diretório para o diretório de dados de backup:

```
cp -arp /opt/netapp/data/* /backup-data
```

5. Se o SE Linux estiver habilitado:

- a. Obtenha o tipo SE Linux para pastas existentes /opt/netapp/data pasta:

```
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. Expandir o tamanho do /opt/netapp/data diretório para um mínimo de 150 GB por meio de comandos LVM ou adicionando discos extras.



Se você criou /opt/netapp/data 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, como `resize` e `extend` pode não funcionar como esperado.

8. Confirme que o /opt/netapp/data o proprietário do diretório (mysql) e o grupo (root) não foram

alterados:

```
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 habilitado, confirme se o contexto para o `/opt/netapp/data` o 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 no banco de dados no futuro.
11. Copie o conteúdo dos dados de backup de volta para o arquivo expandido `/opt/netapp/data` diretório:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Se o SE Linux estiver habilitado, execute o seguinte comando:

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. Inicie o serviço MySQL:

```
systemctl start mysqld
```

14. Após o serviço MySQL ser iniciado, inicie os serviços `ocie` e `ocieau` na ordem mostrada:

```
systemctl start ocie ocieau
```

15. Depois que todos os serviços forem iniciados, exclua a pasta de backup `/backup-data`:

```
rm -rf /backup-data
```

Adicionar espaço ao disco de dados da máquina virtual VMware

Se precisar aumentar a quantidade de espaço no disco de dados para o banco de dados do Unified Manager, você 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.
- Você deve ter as credenciais de usuário de manutenção.

Recomendamos que você faça backup da 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 do 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 ocorreu na sua implantação, aumente o espaço do disco que for maior. O disco de dados sempre terá mais espaço que o outro disco.

2. No cliente vSphere, selecione a máquina virtual Unified Manager e, em seguida, selecione a guia **Console**.
3. Clique na janela do console e 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 Tamanho do Disco de Dados**.

Adicionar espaço à unidade lógica do servidor Microsoft Windows

Se precisar aumentar a quantidade de espaço em disco para o banco de dados do Unified Manager, você poderá adicionar capacidade à unidade lógica na qual o Unified Manager está instalado.

Antes de começar

Você deve ter privilégios de administrador do Windows.

Recomendamos que você faça backup do banco de dados do Unified Manager antes de adicionar espaço em disco.

Passos

1. Efetue login como administrador no servidor Windows no qual você deseja adicionar espaço em disco.
2. Siga o passo 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 Unified Manager está instalado.	Siga os passos do tópico da Microsoft: "Estender um volume básico"
Em um servidor físico, adicione uma unidade de disco rígido.	Siga os passos do tópico da Microsoft: "Adicionando unidades de disco rígido"

Opção	Descrição
Em uma máquina virtual, aumente o tamanho de uma partição de disco.	Siga os passos do tópico VMware: "Aumentando o tamanho de uma partição de disco"

Gerenciar 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 capacidades podem gerenciar os objetos no Unified Manager.

Adicionar usuários

Você pode adicionar usuários locais ou usuários de banco de dados usando a página Usuários. Você também pode adicionar usuários ou grupos remotos que pertencem a um servidor de autenticação. Você pode atribuir funções a esses usuários e, com base nos privilégios das funções, os usuários podem gerenciar os objetos de armazenamento e os dados com o Unified Manager ou visualizar os dados em um banco de dados.

Antes de começar

- Você deve ter a função de Administrador do Aplicativo.
- Para adicionar um usuário ou grupo remoto, você deve ter habilitado a autenticação remota e configurado seu servidor de autenticação.
- Se você planeja configurar a autenticação SAML para que um provedor de identidade (IdP) autentique usuários que acessam a interface gráfica, certifique-se de que esses usuários estejam definidos como usuários "remotos".

O acesso à interface do usuário não é permitido para usuários do tipo "local" ou "manutenção" quando a autenticação SAML está habilitada.

Se você adicionar um grupo do Windows Active Directory, todos os membros diretos e subgrupos aninhados poderão ser autenticados no Unified Manager, a menos que os subgrupos aninhados estejam desabilitados. Se você adicionar um grupo do OpenLDAP ou 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 você deseja adicionar e insira as informações necessárias.

Ao inserir as informações necessárias do usuário, você deve especificar um endereço de e-mail exclusivo para esse usuário. Você deve evitar especificar endereços de e-mail que sejam compartilhados por vários usuários.

4. Clique em **Adicionar**.

Criar um usuário de banco de dados

Para dar suporte a uma conexão entre o Workflow Automation e o Unified Manager, ou para acessar visualizações de banco de dados, você deve primeiro criar um usuário de banco de dados com a função Esquema de Integração ou Esquema de Relatório na interface de usuário da Web do Unified Manager.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Os usuários do banco de dados fornecem integração com o Workflow Automation e acesso a visualizações de banco de dados específicas de relatórios. Os usuários do banco de dados não têm acesso à interface da Web do Unified Manager ou 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 do 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 **Função**, selecione a função apropriada.

Se você é...	Escolha esta função
Conectando o Unified Manager com a automação do fluxo de trabalho	Esquema de Integração
Acessando relatórios e outras visualizações de banco de dados	Esquema de Relatório

6. Clique em **Adicionar**.

Editar as configurações do usuário

Você pode editar as configurações do usuário — como endereço de e-mail e função — especificadas para cada usuário. Por exemplo, você pode querer alterar a função de um usuário que é um operador de armazenamento e atribuir privilégios de administrador de armazenamento ao usuário.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Quando você modifica a função atribuída a um usuário, as alterações são aplicadas quando ocorre uma das seguintes ações:

- O usuário efetua logout e login novamente no Unified Manager.
- O tempo limite da sessão de 24 horas foi atingido.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Usuários**.
2. Na página Usuários, selecione o usuário para o qual você 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**.

Ver usuários

Você pode usar a página Usuários para visualizar a lista de usuários que gerenciam objetos de armazenamento e dados usando o Unified Manager. Você pode visualizar detalhes sobre os usuários, como nome de usuário, tipo de usuário, endereço de e-mail e a função atribuída aos usuários.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Etapas

1. No painel de navegação esquerdo, clique em **Geral > Usuários**.

Excluir usuários ou grupos

Você pode 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 reatribuir os eventos atribuídos aos usuários dos grupos remotos.

Se você estiver excluindo usuários locais ou remotos, os eventos atribuídos a esses usuários serão automaticamente desatribuídos.
- Você deve ter a função de Administrador do Aplicativo.

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 **Sim** para confirmar a exclusão.

O que é RBAC

O RBAC (controle de acesso baseado em função) fornece a capacidade de controlar quem tem acesso a vários recursos e funcionalidades no servidor do Active IQ Unified Manager .

O que o controle de acesso baseado em função faz

O controle de acesso baseado em funções (RBAC) permite que os administradores gerenciem grupos de usuários definindo funções. Se você precisar restringir o acesso a funcionalidades específicas para administradores selecionados, será necessário configurar contas de administrador para eles. Se quiser restringir as informações que os administradores podem visualizar e as operações que eles podem executar, você deve aplicar funções às contas de administrador que criar.

O servidor de gerenciamento usa RBAC para login de usuário e permissões de função. Se você não alterou as configurações padrão do servidor de gerenciamento para acesso de usuário administrativo, não será necessário efetuar login para visualizá-las.

Quando você inicia uma operação que requer privilégios específicos, o servidor de gerenciamento solicita que você faça login. Por exemplo, para criar contas de administrador, você deve fazer login com acesso de conta de administrador do aplicativo.

Definições de tipos de usuários

Um tipo de usuário especifica o tipo de conta que o usuário possui 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 usuários do Unified Manager são os seguintes:

- **Usuário de manutenção**

Criado durante a configuração inicial do Unified Manager. O usuário de manutenção então cria usuários adicionais e atribui funções. O usuário de manutenção também é o único usuário com acesso ao console 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 interface do usuário do Unified Manager e executa funções com base na função atribuída pelo usuário de manutenção ou por um usuário com a função de Administrador do Aplicativo.

- **Grupo remoto**

Um grupo de usuários que acessam a interface do usuário 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 dentro do grupo remoto recebem acesso à interface do usuário do Unified Manager usando suas credenciais de usuário individuais. Grupos remotos podem executar funções de acordo com suas funções atribuídas.

- **Usuário remoto**

Acessa a interface do usuário do Unified Manager usando as credenciais armazenadas no servidor de autenticação. Um usuário remoto executa funções com base na função atribuída pelo usuário de manutenção ou por um usuário com a função de Administrador do Aplicativo.

- **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 ou ao console de manutenção e não pode executar chamadas de API.

Definições de funções de usuário

O usuário de manutenção ou administrador do aplicativo atribui uma função a cada usuário. Cada função contém certos privilégios. O escopo de atividades que você pode executar no Unified Manager depende da função atribuída a você e dos privilégios que a função contém.

O Unified Manager inclui as seguintes funções de usuário predefinidas:

- **Operador**

Visualiza informações do sistema de armazenamento e outros dados coletados pelo Unified Manager, incluindo históricos e tendências de capacidade. Essa função permite que o operador de armazenamento visualize, atribua, reconheça, resolva e adicione notas para os eventos.

- **Administrador de Armazenamento**

Configura operações de gerenciamento de armazenamento no Unified Manager. Essa função permite que o administrador de armazenamento configure limites e crie alertas e outras opções e políticas específicas de gerenciamento de armazenamento.

- **Administrador do aplicativo**

Configura definições não relacionadas ao gerenciamento de armazenamento. Esta função permite o gerenciamento de usuários, certificados de segurança, acesso ao banco de dados e opções administrativas, incluindo autenticação, SMTP, rede e AutoSupport.



Quando o Unified Manager é instalado em sistemas Linux, o usuário inicial com a função de Administrador de Aplicativos é automaticamente nomeado “umadmin”.

- **Esquema de Integração**

Esta função permite acesso somente leitura às visualizações do banco de dados do Unified Manager para integração com o OnCommand Workflow Automation (WFA).

- **Esquema de Relatório**

Essa função permite acesso somente leitura a relatórios e outras visualizações 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_desempenho
- ocum
- ocum_report

- ocum_report_birth
- opm
- monitor de escala

Funções e recursos do usuário do Unified Manager

Com base na função de usuário atribuída a você, você pode determinar quais operações pode executar no Unified Manager.

A tabela a seguir exibe as funções que cada função de usuário pode executar:

Função	Operador	Administrador de Armazenamento	Administrador do aplicativo	Esquema de Integração	Esquema de Relatório
Exibir informações do sistema de armazenamento	•	•	•	•	•
Veja outros dados, como históricos e tendências de capacidade	•	•	•	•	•
Visualizar, atribuir e resolver eventos	•	•	•		
Exibir objetos de serviço de armazenamento, como associações de SVM e pools de recursos	•	•	•		
Ver políticas de limite	•	•	•		
Gerenciar objetos de serviço de armazenamento, como associações SVM e pools de recursos		•	•		

Função	Operador	Administrador de Armazenamento	Administrador do aplicativo	Esquema de Integração	Esquema de Relatório
Definir alertas		•	•		
Gerenciar opções de gerenciamento de armazenamento		•	•		
Gerenciar políticas de gerenciamento de armazenamento		•	•		
Gerenciar usuários			•		
Gerenciar opções administrativas			•		
Definir políticas de limite			•		
Gerenciar acesso ao banco de dados			•		
Gerenciar a integração com o WFA e fornecer acesso às visualizações do banco de dados				•	
Agendar e salvar relatórios		•	•		
Executar operações “Fix It” a partir de Ações de Gerenciamento		•	•		

Função	Operador	Administrador de Armazenamento	Administrador do aplicativo	Esquema de Integração	Esquema de Relatório
Forneça acesso somente leitura às visualizações do banco de dados					•

Gerenciar configurações de autenticação SAML

Depois de configurar as definições de autenticação remota, você pode habilitar a autenticação SAML (Security Assertion Markup Language) para que os usuários remotos sejam autenticados por um provedor de identidade seguro (IdP) antes de poderem acessar a interface de usuário da Web do Unified Manager.

Observe que somente usuários remotos terão acesso à interface gráfica do usuário do Unified Manager após a autenticação SAML ser habilitada. Usuários locais e usuários de manutenção não poderão acessar a interface do usuário. Esta 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.

Você deve inserir o URI e os metadados do Unified Manager no servidor IdP. Você pode copiar essas informações da página Autenticação SAML do Unified Manager. O Unified Manager é considerado o provedor de serviços (SP) no padrão Security Assertion Markup Language (SAML).

Padrões de criptografia suportados

- Padrão de Criptografia Avançada (AES): AES-128 e AES-256
- Algoritmo de Hash Seguro (SHA): SHA-1 e SHA-256

Provedores de identidade validados

- Shibboleth
- Serviços de Federação do Active Directory (ADFS)

Requisitos de configuração do ADFS

- Você deve definir três regras de reivindicação na seguinte ordem que são necessárias para que o Unified Manager analise as respostas SAML do ADFS para esta entrada de confiança da parte confiável.

Regra de reivindicação	Valor
Nome da conta SAM	Nome ID
Nome da conta SAM	urna:oid:0.9.2342.19200300.100.1.1
Grupos de tokens — 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 poderão receber um erro ao efetuar logout do Unified Manager. Siga estes passos:
 - a. Abra o Console de Gerenciamento do ADFS.
 - b. Clique na pasta Políticas de Autenticação na visualização em 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 do padrão “Autenticação do Windows”.
- Em alguns casos, o login pelo IdP é rejeitado quando o certificado de segurança do Unified Manager é assinado pela CA. Há duas soluções alternativas para resolver esse problema:
 - Siga as instruções identificadas no link para desabilitar a verificação de revogação no servidor ADFS para a parte confiável associada ao certificado de CA encadeado:

["Desabilitar verificação de revogação por parte confiável"](#)
 - Faça com que o servidor CA resida no servidor ADFS para assinar a solicitação de certificado do servidor do Unified Manager.

Outros requisitos de configuração

- O desvio de relógio do Unified Manager é definido como 5 minutos, portanto a diferença de tempo entre o servidor IdP e o servidor do Unified Manager não pode ser maior que 5 minutos, ou a autenticação falhará.

Habilitar autenticação SAML

Você pode habilitar a autenticação SAML (Security Assertion Markup Language) para que usuários remotos sejam autenticados por um provedor de identidade seguro (IdP) antes de poderem acessar a interface 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 de 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 habilitar 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 do 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 habilitada. Usuários locais e usuários de manutenção não poderão acessar a interface do usuário. Esta configuração não afeta os usuários que acessam o console de manutenção, os comandos do Unified Manager ou os ZAPIs.



O Unified Manager é reiniciado automaticamente após você concluir a configuração do SAML nesta página.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação SAML**.
2. Marque a caixa de seleção **Ativar autenticação SAML**.

Os campos necessários para configurar a conexão IdP são exibidos.

3. Insira o URI do IdP e os metadados do IdP necessários para conectar o servidor do Unified Manager ao servidor IdP.

Se o servidor IdP estiver acessível diretamente do servidor do Unified Manager, você poderá clicar no botão **Obter metadados do IdP** depois de inserir o URI do IdP para preencher o campo Metadados do 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.

Você pode configurar o servidor IdP com essas informações neste momento.

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 **Confirmar e Sair** e o Unified Manager será reiniciado.

Na próxima vez que 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 tiver 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 seu provedor de identidade, a GUI do Unified Manager não respeita 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 de recursos > 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 esquerdo, clique em **Geral > Autenticação SAML**.
2. Insira o novo URI do IdP e os metadados do IdP necessários para conectar o servidor do Unified Manager ao IdP.

Se o IdP estiver acessível diretamente do servidor do Unified Manager, você poderá clicar no botão **Obter metadados do IdP** depois de inserir o URL do IdP para preencher o campo Metadados do IdP automaticamente.

3. Copie o URI de metadados do Unified Manager ou salve os metadados em um arquivo de texto XML.
4. Clique em **Salvar configuração**.

Uma caixa de mensagem é exibida para confirmar que você deseja 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.

Na próxima vez que 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.

Atualizar as configurações de autenticação SAML após a alteração do certificado de segurança do Unified Manager

Qualquer alteração no certificado de segurança HTTPS instalado no servidor do Unified Manager exige que você atualize as configurações de autenticação SAML. O certificado será 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 do Unified Manager para reativar o acesso à interface do usuário.

Passos

1. Efetue login no console de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

Uma mensagem é exibida para confirmar que você deseja desabilitar a autenticação SAML e reiniciar o Unified Manager.

3. Inicie a interface do usuário do Unified Manager usando o FQDN ou endereço IP atualizado, aceite o certificado do servidor atualizado no seu navegador e efetue login usando as credenciais do usuário de manutenção.
4. Na página **Configuração/Autenticação**, selecione a aba **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 **Confirmar e Sair** e o Unified Manager será reiniciado.
8. Acesse seu servidor IdP e insira o URI e os metadados do servidor do Unified Manager para concluir a configuração.

Provedor de identidade	Etapas de configuração
ADFS	a. Exclua a entrada de confiança da parte confiável existente na GUI de gerenciamento do ADFS. b. Adicione uma nova entrada de confiança de terceira parte confiável usando o <code>saml_sp_metadata.xml</code> do servidor Unified Manager atualizado. c. Defina as três regras de reivindicação necessárias para que o Unified Manager analise as respostas SAML do ADFS para esta entrada de confiança da parte confiável. d. Reinicie o serviço ADFS do Windows.
Shibboleth	a. Atualize o novo FQDN do servidor Unified Manager no <code>attribute-filter.xml</code> e <code>relying-party.xml</code> arquivos. b. Reinicie o servidor web Apache Tomcat e aguarde a porta 8005 ficar online.

9. Efetue login no Unified Manager e verifique se a autenticação SAML funciona conforme o esperado por meio do seu IdP.

Desativar autenticação SAML

Você pode desabilitar a autenticação SAML quando quiser parar de autenticar usuários remotos por meio de um provedor de identidade seguro (IdP) antes que eles possam efetuar login na interface da Web do Unified Manager. Quando a autenticação SAML está desabilitada, os provedores de serviços de diretório configurados, como Active Directory ou LDAP, executam a autenticação de login.

Após desabilitar a autenticação SAML, os usuários locais e de manutenção poderão acessar a interface gráfica do usuário, além dos usuários remotos configurados.

Você também pode desabilitar 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 desabilitada.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Autenticação SAML**.
2. Desmarque a caixa de seleção **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 **Confirmar e Sair** e o Unified Manager será reiniciado.

Na próxima vez que 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.

Desabilitar a autenticação SAML no console de manutenção

Pode ser necessário desabilitar a autenticação SAML no console de manutenção quando não houver acesso à GUI do Unified Manager. Isso pode acontecer em casos de configuração incorreta 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 desabilitada, os provedores de serviços de diretório configurados, como Active Directory ou LDAP, executam a autenticação de login. Usuários locais e usuários de manutenção poderão acessar a interface gráfica do usuário, além dos usuários remotos configurados.

Você também pode desabilitar a autenticação SAML na página Configuração/Autenticação na interface do usuário.



O Unified Manager é reiniciado automaticamente após a autenticação SAML ser desabilitada.

Passos

1. Efetue login no console de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

Uma mensagem é exibida para confirmar que você deseja desabilitar a autenticação SAML e reiniciar o Unified Manager.

3. Digite **y** e pressione Enter para reiniciar o Unified Manager.

Na próxima vez que 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 de 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 interface da Web do Unified Manager.

- Você deve ter a função de Administrador de Aplicativos para criar ou modificar a configuração SAML.
- Você deve ter configurado a autenticação remota.
- Você deve ter configurado pelo menos um usuário remoto ou grupo remoto.

Após a autenticação remota e os usuários remotos terem sido configurados, você pode marcar a caixa de seleção **Habilitar autenticação SAML** para habilitar a autenticação usando um provedor de identidade seguro.

- **URI do IdP**

O URI para acessar o IdP do servidor do Unified Manager. Exemplos de URIs estão listados abaixo.

URI de exemplo do ADFS:

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml
```

Exemplo de URI Shibboleth:

```
https://centos7.ntap2016.local/idp/shibboleth
```

- **Metadados IdP**

Os metadados do IdP em formato XML.

Se o URL do IdP estiver acessível no servidor do Unified Manager, você poderá clicar no botão **Obter metadados do IdP** para preencher este campo.

- **Sistema Host (FQDN)**

O FQDN do sistema host do Unified Manager, conforme definido durante a instalação. Você pode alterar esse valor se necessário.

- **URI do host**

O URI para acessar o sistema host do Unified Manager a partir do IdP.

- **Metadados do host**

Metadados do sistema host em formato XML.

Gerenciar autenticação

Você pode habilitar a autenticação usando LDAP ou Active Directory no servidor do Unified Manager e configurá-lo para funcionar com seus servidores para autenticar usuários remotos.

Para habilitar a autenticação remota, configurar serviços de autenticação e adicionar servidores de autenticação, consulte a seção anterior sobre **Configurando o Unified Manager para enviar notificações de alerta**.

Editar servidores de autenticação

Você pode alterar a porta que o servidor do Unified Manager usa para se comunicar com seu servidor de autenticação.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

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 você deseja editar e clique em **Editar**.
4. Na caixa de diálogo **Editar servidor de autenticação**, edite os detalhes da porta.
5. Clique em **Salvar**.

Excluir 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 você quiser alterar um servidor de autenticação com o qual o servidor de gerenciamento está se comunicando, você pode excluir o servidor de autenticação e adicionar um novo servidor de autenticação.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Quando você exclui um servidor de autenticação, usuários ou grupos remotos 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 **Sim** para confirmar a solicitação de exclusão.

Se a opção **Usar conexão segura** estiver habilitada, os certificados associados ao servidor de autenticação serão excluídos junto com o servidor de autenticação.

Autenticação com Active Directory ou OpenLDAP

Você pode habilitar a autenticação remota no servidor de gerenciamento e configurá-lo 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:

- Diretório Ativo da Microsoft



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 usuários remotos no servidor de autenticação acessem o Unified Manager. As credenciais para usuários ou grupos remotos são mantidas pelo servidor de autenticação. O servidor de gerenciamento usa o Lightweight Directory Access Protocol (LDAP) para autenticar usuários remotos dentro do servidor de autenticação configurado.

Para usuários locais criados no Unified Manager, o servidor de gerenciamento mantém seu próprio banco de dados de nomes de usuários e senhas. O servidor de gerenciamento executa a autenticação e não usa o Active Directory ou o OpenLDAP para autenticação.

Registro de auditoria

Você pode detectar se os logs de auditoria foram comprometidos usando Logs de Auditoria. Todas as atividades realizadas por um usuário são monitoradas e registradas nos Logs de Auditoria. As auditorias são realizadas para todas as funcionalidades da interface do usuário e das APIs expostas publicamente do Active IQ Unified Manager.

Você pode usar o **Registro de auditoria: Visualização de arquivo** para visualizar e acessar todos os arquivos de log de auditoria disponíveis no seu Active IQ Unified Manager. Os arquivos no Log de auditoria: Exibição de arquivos são listados com base na data de criação. Esta exibição exibe informações de todos os logs de auditoria capturados desde a instalação ou atualização até o presente no sistema. Sempre que você executa uma ação no Unified Manager, as informações são atualizadas e ficam disponíveis nos logs. O status de cada arquivo de log é capturado usando o atributo “File Integrity Status”, que é monitorado ativamente para detectar adulteração ou exclusão do arquivo de log. Os logs de auditoria podem ter um dos seguintes estados quando estão disponíveis no sistema:

Estado	Descrição
ATIVO	Arquivo no qual os logs estão sendo registrados atualmente.
NORMAL	Arquivo que está inativo, compactado e armazenado no sistema.
VIOLADO	Arquivo que foi comprometido por um usuário que editou o arquivo manualmente.
EXCLUSÃO_MANUAL	Arquivo que foi excluído por um usuário autorizado.
ROLLOVER_DELETE	Arquivo que foi excluído devido à descontinuação com base na Política de configuração de descontinuação.

Estado	Descrição
EXCLUSÃO_INESPERADA	Arquivo que foi excluído por motivos desconhecidos.

A página Log de Auditoria inclui os seguintes botões de comando:

- Configurar
- Excluir
- Download

O botão **EXCLUIR** permite que você exclua 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 junto com o nome do usuário que executou a operação de exclusão.



A exclusão de um arquivo de log causará a exclusão do arquivo do sistema, mas a entrada na tabela do banco de dados 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 “TAMPERED” são baixados em um formato compactado .gzip formatar.

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 logs de auditoria arquivados não estão incluídos.

Configurar logs de auditoria

Você pode usar o botão **Configurar** na seção Logs de Auditoria para configurar a política contínua para arquivos de Log de Auditoria e também habilitar o registro remoto para os Logs de Auditoria.

Você pode definir os valores em **TAMANHO MÁXIMO DO ARQUIVO** e **DIAS DE RETENÇÃO DO LOG DE AUDITORIA** de acordo com a quantidade e a frequência desejadas de dados que você deseja armazenar no sistema. O valor no campo **TAMANHO TOTAL DO LOG DE AUDITORIA** é o tamanho total dos dados do log de auditoria presentes no sistema. A política de rollover é determinada pelos valores no campo **DIAS DE RETENÇÃO DO LOG DE AUDITORIA**, **TAMANHO MÁXIMO DO ARQUIVO** 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 do arquivo continua disponível no banco de dados e é marcada como “Rollover Delete”. O valor **DIAS DE RETENÇÃO DO LOG DE AUDITORIA** 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 será substituído.

Passos

1. Clique em **Registros de auditoria > > Configurar**.
2. Insira valores em **TAMANHO MÁXIMO DO ARQUIVO**, **TAMANHO TOTAL DO LOG DE AUDITORIA** e

DIAS DE RETENÇÃO DO LOG DE AUDITORIA.

Se você quiser habilitar o registro remoto, selecione **Habilitar registro remoto**. /// 2025-6-11, OUTRODOC-133

Habilitar registro remoto de logs de auditoria

Você pode selecionar a caixa de seleção **Habilitar registro remoto** na caixa de diálogo Configurar registros de auditoria para habilitar o registro de auditoria remota. Você pode usar este 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 caso os arquivos de log de auditoria no servidor Active IQ Unified Manager sejam adulterados.

Passos

1. Na caixa de diálogo **Configurar logs de auditoria**, marque a caixa de seleção **Habilitar registro remoto**.

Campos adicionais para configurar o registro remoto são exibidos.

2. Digite o **HOSTNAME** e a **PORTA** do servidor remoto ao qual você deseja se conectar.
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 formatar. Este certificado deve ser obtido do servidor Syslog de destino e não deve ter expirado. O certificado deve conter o "hostname" selecionado como parte do SubjectAltName Atributo (SAN).

4. Insira os valores para os seguintes campos: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

Os valores devem estar em milissegundos para esses campos.

5. Selecione o formato Syslog necessário e a versão do protocolo TLS nos campos **FORMAT** e **PROTOCOL**.
6. Marque a caixa de seleção **Habilitar 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 ao servidor Syslog antes de salvar a configuração do Log de Auditoria, caso contrário, a conexão falhará. Dependendo do tipo de servidor Syslog, pode ser necessário criar um hash do certificado de autenticação do cliente.

Exemplo: syslog-ng requer que um <hash> do certificado seja criado usando o comando `openssl x509 -noout -hash -in cert.pem`, e então você deve vincular simbolicamente o certificado de autenticação do cliente a um arquivo nomeado após <hash> .0.

7. Clique em **Salvar** para configurar a conexão com seu servidor e habilitar o registro remoto.

Você será redirecionado para a página Logs de Auditoria.



O valor **Tempo limite de conexão** pode afetar a configuração. Se a configuração demorar mais tempo para responder do que o valor definido, isso poderá levar à falha de configuração devido a um erro de conexão. Para estabelecer uma conexão bem-sucedida, aumente o valor **Tempo limite de conexão** e tente a configuração novamente.

Página de autenticação remota

Você pode usar a página Autenticação Remota para configurar o Unified Manager para se comunicar com seu servidor de autenticação para autenticar usuários remotos que tentam fazer login na interface da Web do Unified Manager.

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Depois de marcar a caixa de seleção Habilitar autenticação remota, você pode habilitar a autenticação remota usando um servidor de autenticação.

• Serviço de Autenticação

Permite que você configure o servidor de gerenciamento para autenticar usuários em provedores de serviços de diretório, como Active Directory, OpenLDAP, ou especifique seu próprio mecanismo de autenticação. Você pode especificar um serviço de autenticação somente se tiver habilitado a autenticação remota.

◦ Diretório Ativo

- Nome do Administrador

Especifica o nome do administrador do servidor de autenticação.

- Senha

Especifica a senha para acessar o servidor de autenticação.

- Nome Distinto Base

Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for `ou@domain.com`, o nome distinto base será **cn=ou,dc=domain,dc=com**.

- Desativar pesquisa de grupo aninhado

Especifica se a opção de pesquisa de grupo aninhado deve ser habilitada ou desabilitada. Por padrão, esta opção está desabilitada. Se você usar o Active Directory, poderá acelerar a autenticação desabilitando o suporte para grupos aninhados.

- Usar conexão segura

Especifica o serviço de autenticação usado para comunicação com servidores de autenticação.

◦ OpenLDAP

- Vincular nome distinto

Especifica o nome distinto de vinculação que é usado junto com o nome distinto base para localizar usuários remotos no servidor de autenticação.

- Senha de vinculação

Especifica a senha para acessar o servidor de autenticação.

- Nome Distinto Base

Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for `ou@domain.com`, o nome distinto base será **cn=ou,dc=domain,dc=com**.

- Usar conexão segura

Especifica que o LDAP seguro é usado para comunicação com servidores de autenticação LDAP.

- **Outros**

- Vincular nome distinto

Especifica o nome distinto de vinculação que é usado junto com o nome distinto base para localizar usuários remotos no servidor de autenticação que você configurou.

- Senha de vinculação

Especifica a senha para acessar o servidor de autenticação.

- Nome Distinto Base

Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for `ou@domain.com`, o nome distinto base será **cn=ou,dc=domain,dc=com**.

- Versão do Protocolo

Especifica a versão do Lightweight Directory Access Protocol (LDAP) suportada pelo seu servidor de autenticação. Você pode especificar se a versão do protocolo deve ser detectada automaticamente ou definir a versão como 2 ou 3.

- Atributo de nome de usuário

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 especificados no servidor de autenticação do usuário.

- UGID

Se os usuários remotos forem incluídos como membros de um objeto `GroupOfUniqueNames` no servidor de autenticação, esta opção permitirá que você atribua a associação de grupo do servidor de gerenciamento aos usuários remotos com base em um atributo especificado nesse objeto `GroupOfUniqueNames`.

- Desativar pesquisa de grupo aninhado

Especifica se a opção de pesquisa de grupo aninhado deve ser habilitada ou desabilitada. Por padrão, esta opção está desabilitada. Se você usar o Active Directory, poderá acelerar a autenticação desabilitando o suporte para grupos aninhados.

- **Membro**

Especifica o nome do atributo que seu servidor de autenticação usa para armazenar informações sobre os membros individuais de um grupo.

- **Classe de objeto do usuário**

Especifica a classe de objeto de um usuário no servidor de autenticação remota.

- **Classe de Objeto de Grupo**

Especifica a classe de objeto de todos os grupos no servidor de autenticação remota.



Os valores inseridos para os atributos *Membro*, *Classe de Objeto de Usuário* e *Classe de Objeto de Grupo* devem ser os mesmos adicionados nas configurações do Active Directory, OpenLDAP e LDAP. Caso contrário, a autenticação poderá falhar.

- **Usar conexão segura**

Especifica o serviço de autenticação usado para comunicação com servidores de autenticação.



Se você quiser modificar o serviço de autenticação, certifique-se de excluir todos os servidores de autenticação existentes e adicionar novos servidores de autenticação.

Área de 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 ou grupos remotos são mantidas pelo servidor de autenticação.

- **Botões de comando**

Permite adicionar, editar ou excluir servidores de autenticação.

- **Adicionar**

Permite que você adicione 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 estiver inacessível.

- **Editar**

Permite que você edite as configurações de um servidor de autenticação selecionado.

- **Excluir**

Exclui os servidores de autenticação selecionados.

- **Nome ou endereço IP**

Exibe o nome do host ou endereço IP do servidor de autenticação usado para autenticar o usuário no servidor de gerenciamento.

- **Porta**

Exibe o número da porta do servidor de autenticação.

- **Teste de Autenticação**

Este botão valida a configuração do seu servidor de autenticação autenticando um usuário ou grupo remoto.

Durante o teste, se você especificar apenas o nome do usuário, o servidor de gerenciamento procurará o usuário remoto no servidor de autenticação, mas não autenticará o usuário. Se você especificar o nome de usuário e a senha, o servidor de gerenciamento pesquisará e autenticará o usuário remoto.

Não é possível testar a autenticação se a autenticação remota estiver desabilitada.

Gerenciar certificados de segurança

Você pode configurar HTTPS no servidor do Unified Manager para monitorar e gerenciar seus clusters por meio de uma conexão segura.

Visualizar o certificado de segurança HTTPS

Você pode comparar os detalhes do certificado HTTPS com o certificado recuperado no seu navegador para garantir que a conexão criptografada do seu navegador com o Unified Manager não esteja sendo interceptada.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Visualizar o certificado permite que você verifique o conteúdo de um certificado regenerado ou visualize os Nomes Alt do Assunto (SAN) a partir dos quais você pode acessar o Unified Manager.

Etapa

1. No painel de navegação esquerdo, clique em **Geral > Certificado HTTPS**.

O certificado HTTPS é exibido no topo da página

Se precisar visualizar informações mais detalhadas sobre o certificado de segurança do que as exibidas na página Certificado HTTPS, você poderá visualizar o certificado de conexão no seu navegador.

Baixe 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 para uma Autoridade de Certificação assinar. Um certificado assinado por uma CA ajuda a evitar ataques do tipo man-in-the-middle e fornece melhor proteção de segurança do que um certificado

autoassinado.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Certificado HTTPS**.
2. Clique em **Baixar solicitação de assinatura de certificado HTTPS**.
3. Salve o `<hostname>.csr` arquivo.

Você pode fornecer o arquivo para uma Autoridade de Certificação assinar e depois instalar o certificado assinado.

Instalar um certificado HTTPS assinado e retornado pela CA

Você pode carregar e instalar um certificado de segurança depois que uma Autoridade Certificadora o assinar e devolver. O arquivo que você carrega e instala deve ser uma versão assinada do certificado autoassinado existente. Um certificado assinado por uma CA ajuda a evitar ataques do tipo 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:

- Baixou o arquivo de solicitação de assinatura de certificado e o assinou com uma autoridade de certificação
- Salvou a cadeia de certificados no formato PEM
- Incluiu todos os certificados na cadeia, desde o certificado do servidor do Unified Manager até o certificado de assinatura raiz, incluindo quaisquer certificados intermediários presentes

Você deve ter a função de Administrador do Aplicativo.



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 **Escolher arquivo...** para localizar o arquivo a ser carregado.
4. Selecione o arquivo e clique em **Instalar** para instalar o arquivo.

Para obter informações, consulte ["Instalando um certificado HTTPS gerado usando ferramentas externas"](#).

Exemplo de cadeia de certificados

O exemplo a seguir mostra como o arquivo da 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 autoassinados ou assinados por CA e 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 pares de chaves pública-privada gerados externamente. Os algoritmos de pares 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 enviar deve estar no seguinte formato de entrada.

1. Chave privada do servidor que pertence ao host do 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 usadas para assinar o certificado acima

Formato para carregar um certificado com um par de chaves EC

As curvas permitidas são “prime256v1” e “secp384r1”. Exemplo 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 pertencente 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-----

```

Após o upload do certificado, você deve reiniciar a instância do Active IQ Unified Manager para que as alterações entrem em vigor.

Verificações durante o upload de certificados gerados externamente

O sistema realiza verificações ao carregar um certificado gerado usando ferramentas externas. Se alguma das verificações falhar, o certificado será rejeitado. Também há validação incluída para os certificados gerados a partir do CSR dentro do produto e para certificados gerados usando ferramentas externas.

- A chave privada na entrada é validada em relação ao certificado do host na entrada.
- O Nome Comum (CN) no certificado do host é verificado em relação ao FQDN do host.

- O Nome Comum (CN) do certificado do host não deve estar vazio ou em branco e não deve ser definido como localhost.
- A data de início da validade não deve ser no futuro e a data de expiração da validade do certificado não deve ser no passado.
- Se existir uma CA intermediária ou CA, a data de início da validade do certificado não deve ser no futuro e a data de expiração da 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): https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["O ActiveIQ Unified Manager falha ao instalar um certificado gerado externamente"]

Descrições de páginas para gerenciamento de certificados

Você pode usar a página Certificado HTTPS para visualizar os certificados de segurança atuais e gerar novos certificados HTTPS.

Página do certificado HTTPS

A página Certificado HTTPS permite que você visualize o certificado de segurança atual, baixe uma solicitação de assinatura de certificado, gere um novo certificado HTTPS autoassinado ou instale um novo certificado HTTPS.

Se você não gerou um novo certificado HTTPS autoassinado, o certificado que aparece nesta página é o certificado que foi gerado durante a instalação.

Botões de comando

Os botões de comando permitem que você execute as seguintes operações:

- **Baixar solicitação de assinatura de certificado HTTPS**

Baixa uma solicitação de certificação para o certificado HTTPS instalado no momento. Seu navegador solicita que você salve o arquivo <hostname>.csr para que você possa fornecê-lo a uma Autoridade de Certificação para assinatura.

- **Instalar certificado HTTPS**

Permite que você carregue e instale um certificado de segurança depois que uma Autoridade de Certificação o assinar e devolver. O novo certificado entra em vigor após você reiniciar o servidor de gerenciamento.

- **Regenerar certificado HTTPS**

Permite que você gere um novo certificado HTTPS autoassinado, que substitui o certificado de segurança atual. O novo certificado entrará em vigor após você reiniciar o Unified Manager.

Caixa de diálogo Regenerar certificado HTTPS

A caixa de diálogo Regenerar certificado HTTPS permite que você personalize as informações de segurança e, em seguida, gere um novo certificado HTTPS com essas informações.

As informações atuais do certificado aparecem 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.

Em configurações de alta disponibilidade do Unified Manager, use o endereço IP virtual.

- **E-mail**

Opcional. Um endereço de e-mail para entrar em contato com sua organização; normalmente o endereço de e-mail do administrador do certificado ou do departamento de TI.

- **Empresa**

Opcional. Normalmente, o nome incorporado da sua empresa.

- **Departamento**

Opcional. O nome do departamento da sua empresa.

- **Cidade**

Opcional. A localização da sua empresa na cidade.

- **Estado**

Opcional. Localização do estado ou província, não abreviada, da sua empresa.

- **País**

Opcional. A localização da sua empresa no país. Normalmente, este é 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 host local 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, host local)” se desejar remover as informações de identificação local do campo Nomes alternativos no certificado. Quando esta caixa de seleção estiver marcada, somente o que você inserir no campo será usado no campo Nomes Alternativos. Se deixado em branco, o certificado resultante não terá nenhum campo Nomes Alternativos.

- **TAMANHO DA CHAVE (ALGORITMO DA CHAVE: RSA)**

O algoritmo principal é definido como RSA. Você pode selecionar um dos tamanhos de chave: 2048, 3072 ou 4096 bits. O tamanho padrão da chave é definido como 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 mais informações, consulte ["Gerando certificados HTTPS"](#).

Monitorar e gerenciar armazenamento

Introdução ao Active IQ Unified Manager

O Active IQ Unified Manager (antigo OnCommand Unified Manager) permite que você monitore e gerencie a integridade e o desempenho dos seus sistemas de armazenamento ONTAP a partir de uma única interface.

O Unified Manager fornece os seguintes recursos:

- Descoberta, monitoramento e notificações para sistemas instalados com software ONTAP .
- Painel para mostrar a capacidade, a segurança e a saúde do desempenho do ambiente.
- Alertas, eventos e infraestrutura de limite aprimorados.
- Exibe gráficos detalhados que mostram a atividade da carga de trabalho ao longo do tempo, incluindo IOPS (operações), MBps (taxa de transferência), latência (tempo de resposta), utilização, capacidade de desempenho e taxa de cache.
- Identifica cargas de trabalho que estão usando excessivamente os componentes do cluster e as cargas de trabalho cujo desempenho é afetado pelo aumento da atividade.
- Fornece sugestões de ações corretivas que podem ser executadas para resolver determinados 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 automatizados.
- Capacidade de criar novas cargas de trabalho, como um LUN ou compartilhamento de arquivos, diretamente do Unified Manager e atribuir um Nível de Serviço de Desempenho para definir os objetivos de desempenho e armazenamento para os usuários que acessam o aplicativo usando essa carga de trabalho.

Introdução ao monitoramento de integridade do Active IQ Unified Manager

O Active IQ Unified Manager (antigo OnCommand Unified Manager) ajuda você a monitorar um grande número de sistemas que executam o software ONTAP por meio de uma interface de usuário centralizada. A infraestrutura do servidor do Unified Manager oferece escalabilidade, capacidade de suporte e recursos aprimorados de monitoramento e notificação.

Os principais recursos do Unified Manager incluem monitoramento, alertas, gerenciamento de disponibilidade e capacidade de clusters, gerenciamento de recursos de proteção e agrupamento de dados de diagnóstico e envio para suporte técnico.

Você pode usar o Unified Manager para monitorar seus clusters. Quando ocorrem problemas no cluster, o Unified Manager notifica você sobre os detalhes desses 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 ocorrerem problemas, você seja notificado por e-mail e traps SNMP.

Você pode usar o Unified Manager para gerenciar objetos de armazenamento 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 seus objetos de cluster usando as informações fornecidas nos gráficos de capacidade e integridade do respectivo objeto de cluster.

Capacidade física e lógica

O Unified Manager utiliza os conceitos de espaço físico e lógico usados para objetos de armazenamento ONTAP .

- Capacidade física: Espaço físico refere-se aos blocos físicos de armazenamento usados no volume. A “capacidade física utilizada” é normalmente menor que a capacidade lógica utilizada devido à redução de dados devido a recursos de eficiência de armazenamento (como deduplicação e compactação).
- Capacidade lógica: Espaço lógico refere-se ao espaço utilizável (os blocos lógicos) em um volume. Espaço lógico refere-se a como o espaço teórico pode ser usado, sem levar em conta os resultados de deduplicação ou compactação. “Espaço lógico usado” é o espaço físico usado mais a economia dos recursos de eficiência de armazenamento (como deduplicação e compactação) que foram configurados. Essa medição geralmente parece maior que a capacidade física utilizada porque não reflete a compactação de dados e outras reduções no espaço físico. Assim, a capacidade lógica total pode ser maior que o espaço provisionado.

Unidades de medida de 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 versões anteriores, essas unidades eram exibidas como KB, MB, GB, TB e PB. A partir do ONTAP 9.10.1, eles são exibidos no Unified Manager como KiB, MiB, GiB, TiB e PiB.



As unidades usadas para taxa de transferência continuam sendo quilobytes 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 Unified Manager para ONTAP 9.10.0 e versões anteriores	Unidade de capacidade exibida no Unified Manager para 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
tuberculose	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 (antigo OnCommand Unified Manager) 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 cargas de trabalho que estão usando excessivamente os componentes do cluster e diminuindo o desempenho de outras cargas de trabalho no cluster. Ao definir políticas de limite de desempenho, você também pode especificar valores máximos para determinados contadores de desempenho, para que eventos sejam gerados quando o limite for violado. O Unified Manager alerta você sobre esses eventos de desempenho para que você possa tomar medidas corretivas e trazer o desempenho de volta aos níveis normais de operação. Você pode visualizar e analisar eventos na interface do usuário do Unified Manager.

O Unified Manager monitora o desempenho de dois tipos de cargas de trabalho:

- Cargas de trabalho definidas pelo usuário

Essas cargas de trabalho consistem em volumes FlexVol e FlexGroup que você criou no seu cluster.

- Cargas de trabalho definidas pelo sistema

Essas cargas de trabalho consistem em atividades internas do sistema.

Usar APIs REST do Unified Manager

O Active IQ Unified Manager fornece APIs REST para visualizar informações sobre monitoramento e gerenciamento do seu ambiente de armazenamento. As APIs também permitem provisionar e gerenciar objetos de armazenamento com base em políticas.

Você também pode executar APIs ONTAP em todos os clusters gerenciados ONTAP usando o gateway de API suportado pelo Unified Manager.

Para obter informações sobre APIs REST do Unified Manager, consulte ["Introdução às APIs REST do Active IQ Unified Manager"](#).

O que o servidor Unified Manager faz

A infraestrutura do 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 registro.

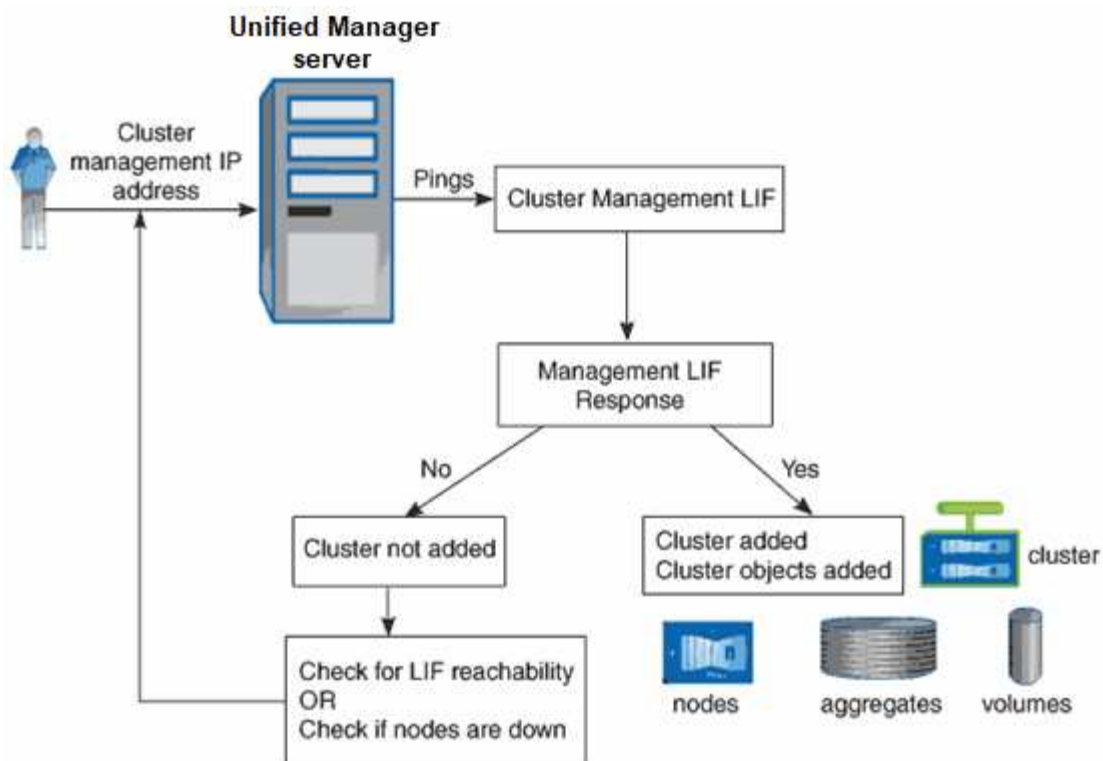
O Unified Manager coleta informações do cluster, armazena os dados no banco de dados e analisa os dados para verificar se há algum problema no cluster.

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 seu banco de dados. Entender como o processo de descoberta funciona ajuda você a gerenciar os clusters da sua organização e seus objetos.

O intervalo de monitoramento padrão é de 15 minutos: se você adicionou um cluster ao servidor do Unified Manager, levará 15 minutos para exibir os detalhes do cluster na interface do usuário do Unified Manager.

A imagem a seguir ilustra o processo de descoberta no Active IQ Unified Manager:



Entenda a interface do usuário

A interface do usuário do Unified Manager consiste principalmente em um painel que fornece uma visão geral dos objetos monitorados. A interface do usuário também fornece acesso à visualização de todos os objetos do cluster.

Você pode selecionar uma visualização preferida e usar os botões de ação conforme necessário. A configuração da sua tela é salva em um espaço de trabalho para que todas as funcionalidades necessárias estejam disponíveis quando você iniciar o Unified Manager. No entanto, quando você navega de uma visualização para outra e depois retorna, a visualização pode não ser a mesma.

Layouts típicos de janelas

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 são semelhantes 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 dos diagramas a seguir.

Layout da janela da lista de objetos

clicar 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 no painel Filtros.

O painel Filtros permite que você filtre 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 que estão offline selecionando a opção de filtro apropriada em Estado.

As colunas relacionadas à capacidade em qualquer lista sempre exibem dados de capacidade em unidades apropriadas, arredondadas para duas casas 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 maiores que 20,45 GB, a capacidade real de 20,454 GB será exibida como 20,45 GB. Da mesma forma, se você filtrar dados menores que 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 exibição Saúde: todos os agregados para filtrar dados maiores que 20,45%, a capacidade real de 20,454% será exibida como 20,45%. Da mesma forma, se você filtrar dados menores que 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 com o mouse.

- **Procurando**

Você pode usar a caixa de pesquisa para procurar determinados atributos de objetos para ajudar a refinar a lista de itens na página de inventário. Por exemplo, você pode digitar "nuvem" para refinar a lista de volumes na página de inventário de volumes e ver todos os volumes que contêm a palavra "nuvem".

- **Exportando dados**

Você pode clicar no botão **Relatórios** (ou no botão **Exportar** para exportar dados para um arquivo de valores separados por vírgulas) (.csv) arquivo, (.pdf) documento ou Microsoft Excel (.xlsx) arquivo e usar os dados exportados para criar relatórios.

Use 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 sumário 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 menu da interface do usuário do Unified Manager.

A ferramenta de busca 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 menu.

Você pode encontrar informações mais detalhadas expandindo qualquer parte do Índice no painel de navegação.

- Para pesquisar o conteúdo da Ajuda, clique na aba **Pesquisar** no painel de navegação, digite a palavra ou série de palavras que deseja encontrar e clique em **Ir!**
- Para imprimir tópicos de Ajuda, clique no ícone da impressora.

Marque seus tópicos de ajuda favoritos

Na aba Favoritos da Ajuda, você pode marcar 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 de Ajuda que você deseja adicionar como favorito.
2. Clique em **Favoritos** e depois em **Adicionar**.

Pesquisar 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 menu. Este método de pesquisa global em todos os objetos permite que você localize 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 "Todos", 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 se restringe aos 25 principais objetos.

Os tipos de objetos que você pode pesquisar incluem:

- Aglomerados
- Nós
- VMs de armazenamento
- Agregados
- Volumes
- Qtrees
- Ações de PMEs
- Ações NFS
- Cotas de usuário ou grupo
- LUNs

- Espaços para nomes NVMe
- Grupos Iniciadores
- Iniciadores
- Grupo de Consistência

Inserir um nome de carga de trabalho retorna a lista de cargas de trabalho na categoria Volumes ou LUNs apropriada.

Você pode clicar em qualquer objeto nos resultados da pesquisa para navegar até a página de detalhes de saúde desse objeto. Se não houver uma página de integridade direta para um objeto, a página de integridade 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.

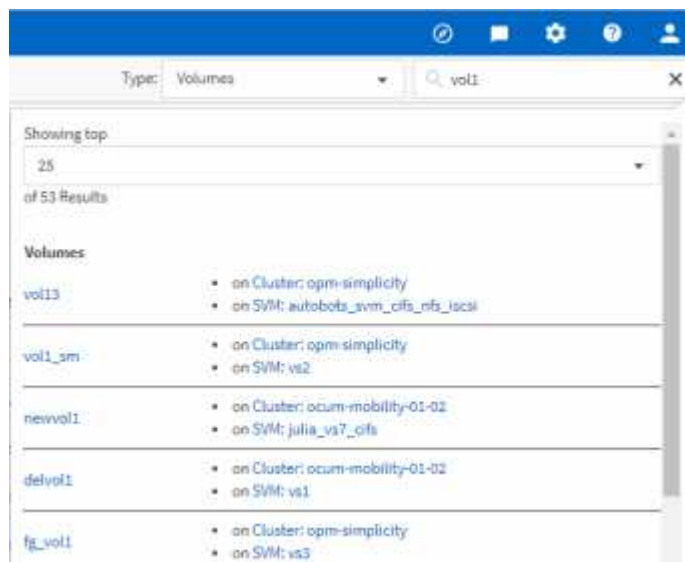


Portas e LIFs não podem ser pesquisadas na barra de pesquisa global.

Passos

1. Selecione um tipo de objeto no menu para refinar os resultados da pesquisa para apenas um único tipo de objeto.
2. Digite no mínimo 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 uma variedade de formatos de saída e então usar os dados exportados para criar relatórios. Por exemplo, se houver 10 eventos críticos que não foram resolvidos, você pode exportar os dados da página de inventário do Gerenciamento de Eventos para criar um relatório e, em seguida, enviá-lo aos 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 use 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 deseja exportar...	Faça isso...
Detalhes do inventário de objetos de armazenamento	Clique em Armazenamento ou Rede no menu de navegação à esquerda e selecione um objeto de armazenamento. Escolha uma das visualizações fornecidas pelo sistema ou qualquer visualização personalizada que você tenha criado.
Detalhes do grupo de política de QoS	Clique em Armazenamento > Grupos de políticas de QoS no menu de navegação à esquerda.
Detalhes do histórico de capacidade de armazenamento e proteção	Clique em Armazenamento > Agregados ou Armazenamento > Volumes e selecione um único agregado ou volume.
Detalhes do evento	Clique em Gerenciamento de eventos no menu de navegação à esquerda.
Detalhes de desempenho dos 10 principais objetos de armazenamento	Clique em Armazenamento > Clusters > Desempenho: Todos os clusters , selecione um cluster e escolha a guia Melhores desempenhos . Em seguida, selecione um objeto de armazenamento e um contador de desempenho.

2. Clique no botão **Relatórios** (ou no botão **Exportar** em algumas páginas da interface do usuário).
3. Clique em **Baixar CSV**, **Baixar PDF** ou **Baixar Excel** para confirmar a solicitação de exportação.

Na guia Melhores Desempenhos, você pode escolher baixar um relatório das estatísticas do cluster único que está visualizando ou de todos os clusters no data center.

O arquivo foi baixado.

4. Abra o arquivo no aplicativo apropriado.

Informações relacionadas

["Página de inventário de saúde/clusters"](#)

["Agendando um relatório"](#)

Filtrar conteúdo da página de inventário

Você pode filtrar dados da página de inventário no Unified Manager para localizar dados rapidamente com base em critérios específicos. Você pode usar a filtragem para

restringir o conteúdo das páginas do Unified Manager e 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 **Filtragem** para personalizar a visualização em grade com base em suas preferências. As opções de filtro disponíveis são baseadas no tipo de objeto visualizado na grade. Se filtros estiverem aplicados no momento, o número de filtros aplicados será exibido à direita do botão Filtro.

Três tipos de parâmetros de filtro são suportados.

Parâmetro	Validação
String (texto)	Os operadores são contém , começa com , termina com e não contém .
Número	Os operadores são maior que , menor que , no último e entre .
Enum (texto)	Os operadores são is e is not .

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 quatro. Os resultados filtrados são baseados em parâmetros de filtro combinados. Os resultados filtrados se aplicam a todas as páginas da sua pesquisa filtrada, não apenas à página exibida no momento.

Você pode adicionar filtros usando o painel Filtragem.

1. No topo da página, clique no botão **Filtro**. O painel Filtragem é exibido.
2. Clique na lista suspensa à esquerda e selecione um objeto; por exemplo, *Cluster* ou um contador de desempenho.
3. Clique na lista suspensa central e selecione o operador que deseja usar.
4. Na última lista, selecione ou insira um valor para completar o filtro para aquele objeto.
5. Para adicionar outro filtro, clique em **+Adicionar filtro**. Um campo de filtro adicional é exibido. Complete este filtro usando o processo descrito nas etapas anteriores. Observe que ao adicionar seu quarto filtro, o botão **+Adicionar Filtro** não será mais exibido.
6. Clique em **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 **Redefinir** 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				
				Cancel Apply Filter

Após clicar em **Aplicar filtro**, o painel Filtragem fecha, aplica seus filtros e mostra o número de filtros aplicados (3).

Visualizar eventos ativos no sino de notificação

O sino de notificação () na barra de menu fornece uma maneira rápida de visualizar 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 7 dias anteriores e não inclui eventos informativos. Você pode clicar em um link para exibir a lista de eventos nos quais você está mais interessado.

Observe que quando um cluster não está acessível, o Unified Manager exibe essas informações nesta página. Você pode visualizar informações detalhadas sobre um cluster inacessível clicando no botão **Detalhes**. Esta ação abre a página Detalhes do evento. Problemas de monitoramento de escala, como pouco espaço ou RAM na estação de gerenciamento, também são exibidos nesta página.

Passos

1. Na barra de menu, clique em .
2. Para ver detalhes de qualquer um dos eventos ativos, clique no link de texto do evento, como "Capacidade para 2 pessoas" ou "Apresentação para 4 pessoas".

Monitore e gerencie clusters no painel

O painel fornece informações cumulativas e rápidas sobre a integridade atual dos seus sistemas ONTAP monitorados. O painel 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 do usuário do Unified Manager, em vez de ter que usar o ONTAP System Manager ou o ONTAP CLI.

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 depois detalhar clusters individuais quando quiser visualizar informações detalhadas.



Alguns dos painéis listados abaixo podem não aparecer na página com base na sua configuração.

Painéis	Descrição
Ações de Gestão	Quando o Unified Manager consegue diagnosticar e determinar uma única resolução para um problema, essas resoluções são exibidas neste painel com um botão Corrigir .
Capacidade	Exibe a capacidade total e utilizada para o nível local e o nível de nuvem, e o número de dias até que a capacidade local atinja o limite superior.
Capacidade de Desempenho	Exibe o valor da capacidade de desempenho para cada cluster e o número de dias até que a capacidade de desempenho atinja o limite superior.
Carga de trabalho IOPS	Exibe o número total de cargas de trabalho que estão sendo executadas em um determinado intervalo de IOPS.
Desempenho da carga de trabalho	Exibe o número total de cargas de trabalho em conformidade e não em conformidade atribuídas a cada Nível de Serviço de Desempenho definido.
Segurança	Exibe o número de clusters que estão em conformidade ou não, o número de SVMs que estão em conformidade ou não e o número de volumes que estão criptografados ou não criptografados.
Proteção	Exibe o número de VMs de armazenamento protegidas pelo relacionamento SVM-DR, volumes protegidos pelo relacionamento SnapMirror, volumes protegidos pelo Snapshot e clusters protegidos pelo MetroCluster.
Visão geral do uso	Exibe clusters classificados pelo maior IOPS, maior taxa de transferência (MBps) ou maior capacidade física utilizada.

Página do painel

A página Painel tem "painéis" que exibem a capacidade de alto nível, o desempenho e a integridade da segurança dos clusters que você está monitorando. Esta página também fornece um painel Ações de Gerenciamento que lista 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 últimas 24 horas. Essas informações ajudam você a decidir quais clusters você pode precisar analisar mais detalhadamente 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 naquela 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 depois detalhar clusters individuais quando quiser visualizar informações detalhadas.



Alguns dos painéis listados abaixo aparecem no painel com base na sua configuração.

Painel de Ações de Gestão

Há certos problemas que o Unified Manager pode diagnosticar completamente e fornecer uma única resolução. Quando disponíveis, essas resoluções são exibidas neste painel com um botão **Corrigir** ou **Corrigir tudo**. Você pode corrigir esses problemas imediatamente no Unified Manager em vez de ter que usar o ONTAP System Manager ou o ONTAP CLI. Para visualizar todas as edições, clique em Ver "[Corrija problemas do ONTAP diretamente do Unified Manager](#)" para mais informações.

Painel de capacidade

Ao visualizar todos os clusters, este painel exibe a capacidade física utilizada (após aplicar economias de eficiência de armazenamento) e a capacidade física disponível (sem incluir economias potenciais de eficiência de armazenamento) para cada cluster, o número de dias até que os discos sejam projetados para ficarem cheios e a taxa de redução de dados (sem cópias de instantâneo) com base nas configurações de eficiência de armazenamento do ONTAP. Ele também lista a capacidade usada para quaisquer níveis de nuvem configurados. Clicar no gráfico de barras leva você para a página de inventário de agregados daquele cluster. Clicar no texto "Dias para atingir a capacidade máxima" 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 visualizar um único cluster, este painel exibe a capacidade física utilizada e a capacidade física disponível para os agregados de dados classificados por cada tipo de disco individual na camada local e na camada de nuvem. Clicar no gráfico de barras de um tipo de disco leva você à página de inventário de volumes que usam esse tipo de disco.

Painel de capacidade de desempenho

Ao visualizar todos os clusters, este painel exibe o valor da capacidade de desempenho de cada cluster (média da última hora) 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 para a página de inventário de nós daquele cluster. Observe que a página de inventário de nós exibe a capacidade de desempenho média das últimas 72 horas. Clicar no texto "Dias para atingir a capacidade máxima" 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 visualizar um único cluster, este painel exibe a porcentagem de capacidade de desempenho do cluster utilizada, os valores de IOPS total e taxa de transferência total (MB/s), além do número de dias até que cada uma dessas três métricas atinja seu limite superior.

Painel IOPS de carga de trabalho

Ao visualizar um único cluster, este painel exibe o número total de cargas de trabalho que estão sendo executadas em um determinado intervalo de IOPS e indica o número para cada tipo de disco quando você passa o cursor sobre o gráfico.

Painel de desempenho da carga de trabalho

Este painel exibe o número total de cargas de trabalho em conformidade e não em conformidade atribuídas a cada política de Nível de Serviço de Desempenho (PSL). Ele também exibe o número de cargas de trabalho

que não têm um PSL atribuído. Clicar em um gráfico de barras leva você às cargas de trabalho em conformidade atribuídas àquela política na página Cargas de trabalho. Clicar no número que segue o gráfico de barras leva você às cargas de trabalho em conformidade e não conformidade atribuídas àquela 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 sua visualização atual. Este painel exibe:

- uma lista dos eventos de segurança recebidos nas últimas 24 horas. Clique em um evento para ver os detalhes na página Detalhes do evento
- o status de segurança do cluster (contagem de clusters compatíveis e não compatíveis)
- o status de segurança da VM de armazenamento (contagem de VMs de armazenamento compatíveis e não compatíveis)
- o status de criptografia do volume (contagem dos volumes criptografados ou não criptografados)
- o status do volume anti-ransomware (contagem de volumes com anti-ransomware que estão habilitados ou desabilitados)

Você pode clicar nos gráficos de barras dos clusters compatíveis e não compatíveis, VMS de armazenamento, volumes criptografados e não criptografados e status anti-ransomware do volume para acessar as respectivas páginas e visualizar os detalhes de segurança dos clusters filtrados, VMs de armazenamento e volumes.

A conformidade é baseada na ["Guia de reforço de segurança da NetApp para ONTAP 9"](#). Clique na seta para a direita na parte superior do painel para visualizar detalhes de segurança de todos os clusters na página Segurança. Para obter informações, consulte ["Visualizando o status de segurança detalhado para clusters e VMs de armazenamento"](#).

Painel de Proteção de Dados

Este painel exibe o resumo da proteção de dados para um ou todos os clusters em um data center. Ele exibe o número total de eventos de proteção de dados, eventos do MetroCluster e número de eventos ativos gerados nas últimas 24 horas no ONTAP. Clicar no link de cada um desses eventos leva você para a página de detalhes do evento. Você pode clicar no link **Exibir tudo** para visualizar todos os eventos de proteção ativos na página de inventário do Gerenciamento de eventos. O painel exibe:

- O número de volumes em um cluster ou todos os clusters em um data center protegidos por cópias de Snapshot.
- O número de volumes em um cluster ou todos os clusters em um data center protegidos por relacionamentos SnapMirror. Para relacionamentos SnapMirror, a contagem de volumes no cluster de origem é considerada.
- O número de clusters ou todos os clusters em um data center protegidos pela configuração do MetroCluster sobre IP ou FC.
- O número de relacionamentos de volume com o objetivo do ponto de recuperação (RPO) do SnapMirror varia com base no status do atraso.

Você pode passar o mouse para visualizar as respectivas contagens e legendas. Você pode clicar na seta para a direita na parte superior do painel para visualizar os detalhes de um ou de todos os clusters na página Proteção de Dados. Você também pode clicar em:

- Os gráficos de barras para volumes desprotegidos e volumes protegidos por cópias de Snapshot permitem acessar a página Volumes e visualizar os detalhes.

- Os gráficos de barras para os clusters protegidos ou não protegidos pela configuração do MetroCluster permitem acessar a página Clusters e visualizar os detalhes.
- Os gráficos de barras de todos os relacionamentos vão para a página Relacionamentos, onde os detalhes são filtrados com base no cluster de origem.

Para mais informações, consulte ["Visualizando o status de proteção do volume"](#).

Painel Visão geral de uso

Ao visualizar todos os clusters, você pode optar por visualizá-los classificados pelo maior IOPS, maior taxa de transferência (MB/s) ou maior capacidade física utilizada.

Ao visualizar um único cluster, você pode optar por visualizar cargas de trabalho classificadas pelo maior IOPS, maior taxa de transferência (MB/s) ou maior capacidade lógica utilizada.

Informações relacionadas

["Corrigindo problemas usando remediações automáticas do Unified Manager"](#)

["Exibindo informações sobre eventos de desempenho"](#)

["Gerenciando o desempenho usando a capacidade de desempenho e as informações de IOPS disponíveis"](#)

["Página de detalhes de volume/saúde"](#)

["Análise e notificação de eventos de desempenho"](#)

["Descrição dos tipos de gravidade do evento"](#)

["Fontes de eventos de desempenho"](#)

["Gerenciar objetivos de segurança do cluster"](#)

["Monitore o desempenho do cluster na página inicial do Performance Cluster"](#)

["Monitore o desempenho usando as páginas do Inventário de Desempenho"](#)

Gerencie problemas ou recursos do ONTAP diretamente do Unified Manager

Você pode corrigir determinados problemas do ONTAP ou gerenciar determinados recursos do ONTAP diretamente da interface de usuário do Unified Manager, em vez de ter que usar o ONTAP System Manager ou o ONTAP CLI. A opção “Ações de gerenciamento” fornece correções para uma série de 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 no Painel, na página Detalhes do Evento e na seleção Análise de Carga de Trabalho no menu de navegação à esquerda.

Há certos problemas que o Unified Manager pode diagnosticar completamente e fornecer uma única resolução. Para determinados recursos do ONTAP, como monitoramento anti-ransomware, o Unified Manager realiza verificações internas e recomenda ações específicas. Quando disponíveis, essas resoluções são exibidas em Ações de gerenciamento com um botão **Corrigir**. Clique no botão **Corrigir** para corrigir o

problema. Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

O Unified Manager envia comandos ONTAP ao cluster para fazer a correção solicitada. Quando a correção estiver concluída, o evento ficará obsoleto.

Algumas ações de gerenciamento permitem que você corrija o mesmo problema em vários objetos de armazenamento usando o botão **Corrigir tudo**. Por exemplo, pode haver 5 volumes com o evento "Espaço de Volume Cheio", que pode ser resolvido clicando na ação de gerenciamento **Corrigir Tudo** para "Habilitar crescimento automático de volume". Com um clique você pode corrigir esse problema em 5 volumes.

Para obter informações sobre os problemas e recursos do ONTAP que você pode gerenciar usando a correção automática, consulte ["Quais problemas o Unified Manager pode corrigir"](#).

Quais opções tenho quando vejo o botão **Corrigir** ou **Corrigir tudo**

A página Ações de gerenciamento fornece o botão **Corrigir** ou **Corrigir tudo** 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 não tiver certeza de que deseja resolver o problema conforme recomendado pelo Unified Manager, você pode executar as seguintes ações:

O que você quer fazer?	Ação
Peça ao Unified Manager para corrigir o problema em todos os objetos identificados.	Clique no botão Corrigir tudo .
Não corrija o problema para nenhum dos objetos identificados neste momento e oculte esta ação de gerenciamento até que o evento seja gerado novamente.	Clique na seta para baixo e clique em Descartar tudo .
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 de Corrigir . Em seguida, siga as etapas para corrigir ou descartar ações de gerenciamento individuais.

O que você quer fazer?	Ação
Peça ao Unified Manager para corrigir o problema.	Clique no botão Corrigir .
Não corrija o problema neste momento e oculte esta ação de gerenciamento até que o evento seja gerado novamente.	Clique na seta para baixo e clique em Descartar .

O que você quer fazer?	Ação
Exiba os detalhes deste evento para que você possa entender melhor o problema.	• Clique no botão Corrigir e revise a correção que será aplicada na caixa de diálogo resultante. • Clique na seta para baixo e clique em Exibir detalhes do evento para exibir a página de detalhes do evento. Em seguida, clique em Corrigir em qualquer uma dessas páginas resultantes se quiser corrigir o problema.
Exiba os detalhes deste 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 Detalhes de integridade.

Em alguns casos, a correção é refletida na próxima pesquisa de configuração de 15 minutos. Em outros casos, pode levar muitas horas para que a alteração de configuração seja verificada e o evento se torne obsoleto.

Para ver a lista de ações de gerenciamento concluídas ou em andamento, clique no ícone de filtro e selecione **Concluídas** ou **Em andamento**.

Corrigir Todas as operações são executadas em série, então quando você visualiza 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.

Visualize o status das ações de gerenciamento que você escolheu corrigir

Você pode visualizar o status de todas as ações de gerenciamento que você escolheu corrigir na página Ações de gerenciamento. A maioria das ações é mostrada como **Concluída** rapidamente depois que o Unified Manager envia o comando ONTAP ao cluster. No entanto, algumas ações, como mover um volume, podem demorar mais.

Há três filtros disponíveis na página Ações de gerenciamento:

- **Concluído** mostra as ações de gerenciamento que foram concluídas com sucesso e aquelas que falharam. Ações **falhadas** fornecem um motivo para a falha para que você possa resolver o problema manualmente.
- **Em andamento** mostra as ações de gerenciamento que estão sendo implementadas e aquelas que estão programadas para serem implementadas.
- **Recomendado** mostra todas as ações de gerenciamento que estão atualmente ativas para todos os clusters monitorados.

Passos

1. Clique em **Ações de gerenciamento** no painel de navegação esquerdo. Alternativamente, clique em  na parte superior do painel **Ações de gerenciamento** no **Painel** e selecione a visualização que deseja ver.

A página Ações de gerenciamento é exibida.

2. Você pode clicar no ícone de acento circunflexo ao lado da ação de gerenciamento no campo **Descrição** para ver detalhes sobre o problema e o comando que está sendo usado para corrigi-lo.
3. Para visualizar quaisquer ações que **falharam**, classifique pela coluna **Status** na Visualização **Concluídas**. Você pode usar a ferramenta **Filtro** para o mesmo propósito.
4. Se quiser ver mais informações sobre uma ação de gerenciamento com falha ou se decidir corrigir uma ação de gerenciamento recomendada, clique em **Exibir detalhes do evento** na área expandida depois de clicar no ícone de circunflexo ao lado da ação de gerenciamento. Um botão **Corrigir** está disponível nessa página.

Quais problemas o Unified Manager pode corrigir

Ao usar o recurso de correção automática do Active IQ Unified Manager, você pode optar por resolver determinados problemas do ONTAP ou gerenciar determinados 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 **Corrigir** ou **Corrigir tudo** na interface da Web do Unified Manager.

Nome e descrição do evento	Ação de Gestão	Operação "Consertar"
Volume Espaço Cheio O volume está quase sem espaço e ultrapassou o limite de capacidade máxima. Este limite é definido por padrão como 90% do tamanho do volume.	Habilitar crescimento automático de volume	O Unified Manager determina que o crescimento automático de volume não está configurado para este volume, então ele habilita esse recurso para que o volume aumente em capacidade quando necessário.
Inodes completos Este volume ficou sem inodes e não pode aceitar novos arquivos.	Aumentar o número de inodes no volume	Aumenta o número de inodes no volume em 2%.
Incompatibilidade de política de nível de armazenamento detectada O volume tem muitos dados inativos e a política de hierarquização atual está definida como "somente instantâneo" ou "nenhum".	Habilitar hierarquização automática da nuvem	Como o volume já reside em um FabricPool, ele altera a política de camadas para "automática" para que os dados inativos sejam movidos para a camada de nuvem de menor custo.
Incompatibilidade de nível de armazenamento detectada O volume tem muitos dados inativos, mas não reside em uma camada de armazenamento habilitada para nuvem (FabricPool).	Alterar nível de armazenamento dos volumes	Move o volume para a camada de armazenamento habilitada para nuvem e define a política de camadas como "automática" para mover dados inativos para a camada de nuvem.

Nome e descrição do evento	Ação de Gestão	Operação "Consertar"
Log de auditoria desabilitado O log de auditoria não está habilitado para a VM de armazenamento	Habilitar registro de auditoria para a VM de armazenamento	Habilita o registro de auditoria na VM de armazenamento. Observe que a VM de armazenamento já deve ter um local de log de auditoria local ou remoto configurado.
Banner de login desabilitado O banner de login do cluster deve ser habilitado para aumentar a segurança, deixando claras as restrições de acesso.	Definir banner de login para o cluster	Define o banner de login do cluster como "Acesso restrito a usuários autorizados".
Banner de login desabilitado O banner de login para a VM de armazenamento deve ser habilitado para aumentar a segurança, deixando claras as restrições de acesso.	Definir banner de login para a VM de armazenamento	Define o banner de login da VM de armazenamento como "Acesso restrito a usuários autorizados".
SSH está usando cifras inseguras Cifras com o sufixo "-cbc" são consideradas inseguras.	Remover cifras inseguras do cluster	Remove as cifras inseguras — como aes192-cbc e aes128-cbc — do cluster.
SSH está usando cifras inseguras Cifras com o sufixo "-cbc" são consideradas inseguras.	Remover cifras inseguras da VM de armazenamento	Remove as cifras inseguras — como aes192-cbc e aes128-cbc — da VM de armazenamento.
Transporte HTTPS de AutoSupport desabilitado O protocolo de transporte usado para enviar mensagens do AutoSupport ao suporte técnico deve ser criptografado.	Defina HTTPS como o protocolo de transporte para mensagens do AutoSupport	Define HTTPS como o protocolo de transporte para mensagens do AutoSupport no cluster.

Nome e descrição do evento	Ação de Gestão	Operação "Consertar"
Limite de desequilíbrio de carga do cluster violado Indica que a carga está desequilibrada entre os nós do cluster. Este evento é gerado quando a variação da capacidade de desempenho utilizada é maior que 30% entre os nós.	Balancear cargas de trabalho do cluster	O Unified Manager identifica o melhor volume para mover de um nó para outro para reduzir o desequilíbrio e, em seguida, move o volume.
Limite de desequilíbrio de capacidade do cluster violado Indica que a capacidade está desequilibrada entre os agregados no cluster. Este evento é gerado quando a variação da capacidade utilizada é maior que 70% entre os agregados.	Capacidade do cluster de equilíbrio	O Unified Manager identifica o melhor volume a ser movido de um agregado para outro para reduzir o desequilíbrio e, em seguida, move o volume.
Limite de capacidade de desempenho usado violado Indica que a carga no nó pode ficar superutilizada se você não reduzir a utilização de uma ou mais cargas de trabalho altamente ativas. Este evento é gerado quando o valor da capacidade de desempenho do nó utilizada é maior que 100% por mais de 12 horas.	Limitar carga alta no nó	O Unified Manager identifica o volume com o maior IOPS e aplica uma política de QoS usando os níveis históricos esperados e de pico de IOPS para reduzir a carga no nó.
Limite de alerta de evento dinâmico violado Indica que o nó já está operando em um estado sobrecarregado devido à carga anormalmente alta de algumas das cargas de trabalho.	Reduzir sobrecarga no nó	O Unified Manager identifica o volume com o maior IOPS e aplica uma política de QoS usando os níveis históricos esperados e de pico de IOPS para reduzir a carga no nó.
A aquisição não é possível O failover está desabilitado no momento, então o acesso aos recursos do nó durante uma interrupção ou reinicialização seria perdido até que o nó ficasse disponível novamente.	Habilitar 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 "Consertar"
A opção Cf.takeover.on_panic está configurada como DESLIGADA A opção nodeshell "cf.takeover.on_panic" está definida como off, o que pode causar um problema em sistemas configurados com HA.	Habilitar aquisição em caso de pânico	O Unified Manager envia o comando apropriado ao cluster para alterar essa configuração para ativado .
Desabilitar a opção snapmirror.enable do nodeshell A antiga opção do nodeshell "snapmirror.enable" está definida como on, o que pode causar um problema durante a inicialização após a atualização para o ONTAP 9.3 ou superior.	Defina a opção snapmirror.enable como desativada	O Unified Manager envia o comando apropriado ao cluster para alterar essa configuração para desativado .
Telnet habilitado Indica um possível problema de segurança porque o Telnet não é seguro e transmite dados de maneira não criptografada.	Desativar Telnet	O Unified Manager envia o comando apropriado ao cluster para desabilitar o Telnet.
Configurar aprendizado anti-ransomware de VM de armazenamento Verifica periodicamente clusters com licenças para monitoramento anti-ransomware. Valida se uma VM de armazenamento suporta apenas volumes NFS ou SMB em tal cluster.	Coloque as VMs de armazenamento em um <code>learning</code> modo de monitoramento anti-ransomware	O Unified Manager define o monitoramento anti-ransomware para <code>learning</code> estado para as VMs de armazenamento por meio do console de gerenciamento do cluster. O monitoramento anti-ransomware em todos os novos volumes criados na VM de armazenamento é movido automaticamente para um modo de aprendizado. Por meio dessa capacitação, o ONTAP pode aprender o padrão de atividade nos volumes e detectar anomalias devido a possíveis ataques maliciosos.

Nome e descrição do evento	Ação de Gestão	Operação "Consertar"
Configurar aprendizado anti-ransomware de volume Verifica periodicamente clusters com licenças para monitoramento anti-ransomware. Valida se um volume suporta apenas serviços NFS ou SMB em tal cluster.	Coloque volumes em <code>learning</code> modo de monitoramento anti-ransomware	O Unified Manager define o monitoramento anti-ransomware para <code>learning</code> estado dos volumes por meio do console de gerenciamento do cluster. Por meio dessa capacitação, o ONTAP pode aprender o padrão de atividade nos volumes e detectar anomalias devido a possíveis ataques maliciosos.
Habilitar volume anti-ransomware Verifica periodicamente clusters com licenças para monitoramento anti-ransomware. Detecta se os volumes estão no <code>learning</code> modo de monitoramento anti-ransomware por mais de 45 dias e determina a perspectiva de colocá-los no modo ativo.	Coloque volumes em <code>active</code> modo de monitoramento anti-ransomware	O Unified Manager define o monitoramento anti-ransomware para <code>active</code> nos volumes por meio do console de gerenciamento do cluster. Por meio dessa habilitação, o ONTAP pode aprender o padrão de atividade nos volumes e detectar anomalias devido a possíveis ataques maliciosos, além de criar alertas para ações de proteção de dados.
Desativar volume anti-ransomware Verifica periodicamente clusters com licenças para monitoramento anti-ransomware. Detecta notificações repetitivas durante o monitoramento anti-ransomware ativo nos volumes (por exemplo, vários avisos de possíveis ataques de ransomware são retornados ao longo de 30 dias).	Desabilitar monitoramento anti-ransomware em volumes	O Unified Manager desabilita o monitoramento anti-ransomware nos volumes por meio do console de gerenciamento do cluster.

Substituir ações de gerenciamento por meio de scripts

Você pode criar scripts personalizados e associá-los a alertas para executar 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 do recurso de ação de gerenciamento fornecido pelo Unified Manager, poderá configurar um script personalizado para a ação específica. Você pode então 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.

Gerenciar clusters

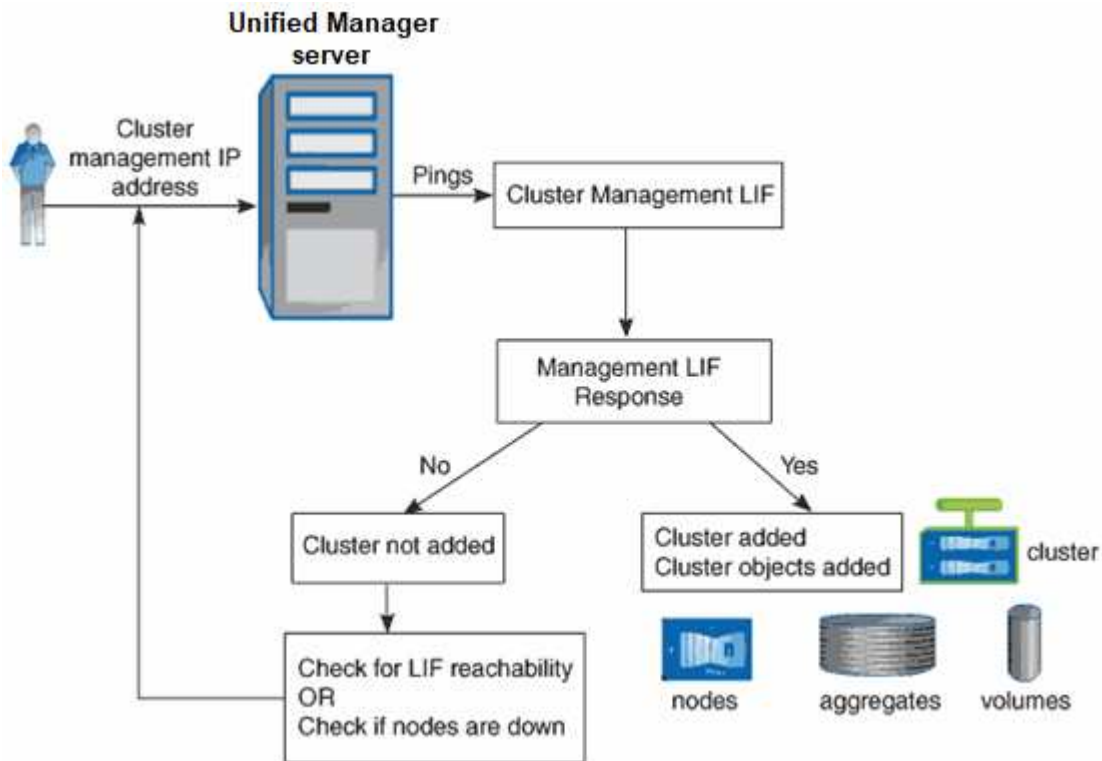
Você pode gerenciar os clusters ONTAP usando o Unified Manager para monitorar, adicionar, editar e remover clusters.

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 seu banco de dados. Entender como o processo de descoberta funciona ajuda você a gerenciar os clusters da sua organização e seus objetos.

O intervalo de monitoramento para coleta de informações de configuração do cluster é de 15 minutos. Por exemplo, depois de adicionar um cluster, leva 15 minutos para exibir os objetos do cluster na interface do usuário do Unified Manager. Esse período também é válido ao fazer alterações em um cluster. Por exemplo, se você adicionar dois novos volumes a uma SVM em um cluster, verá esses novos objetos na interface do usuário após o próximo intervalo de pesquisa, 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 são descobertos, o Unified Manager começa a coletar dados históricos de desempenho dos 15 dias anteriores. Essas estatísticas são coletadas usando a funcionalidade de coleta de continuidade de dados. Este recurso fornece mais de duas semanas de informações de desempenho para um cluster imediatamente após ele 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 15 dias de dados de desempenho exige muita CPU, é recomendável escalonar a adição de novos clusters para que as pesquisas de coleta de continuidade de dados não sejam executadas em muitos clusters ao mesmo tempo.

Ver a lista de clusters monitorados

Você pode usar a página Configuração do Cluster para visualizar seu inventário de clusters. Você pode visualizar detalhes sobre os clusters, como nome ou endereço IP e status de comunicação.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Etapas

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de cluster**.

Todos os clusters no seu ambiente de armazenamento gerenciado pelo Unified Manager são exibidos. A lista de clusters é classificada pela coluna de nível de gravidade do estado da coleção. Você pode clicar em um cabeçalho de coluna para classificar os clusters por colunas diferentes.

Adicionar clusters

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

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou a função de Administrador de Armazenamento.
- Você deve ter as seguintes informações:
 - O Unified Manager oferece suporte a clusters ONTAP locais, ONTAP Select e Cloud Volumes ONTAP.
 - Você deve ter o nome do host ou o endereço IP de gerenciamento do cluster (IPv4 ou IPv6) para o cluster.

Ao usar o nome do host, ele deve ser resolvido para o endereço IP de gerenciamento do cluster para o LIF de gerenciamento do cluster. Se você usar um LIF de gerenciamento de nó, a operação falhará.

- Você deve ter o nome de usuário e a senha para acessar o cluster.

Esta 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 porta 443).
- O cluster deve estar executando o software ONTAP versão 9.9 ou superior.
- Você deve ter espaço adequado no servidor do Unified Manager. Você não poderá adicionar um cluster ao servidor quando mais de 90% do espaço já estiver consumido.

- Você possui os certificados necessários:

Certificado SSL (HTTPS): Este certificado é de propriedade do Unified Manager. Um certificado SSL autoassinado padrão (HTTPS) é gerado com uma nova instalação do Unified Manager. A NetApp recomenda que você atualize para um certificado assinado por CA para maior 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 a regeneração do certificado SSL, consulte ["Gerando um certificado de segurança HTTPS"](#).

Certificado EMS: Este certificado é de propriedade do Unified Manager. 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 habilitada 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 será habilitada.

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



- Você pode adicionar um cluster a partir da interface da web, e a autenticação baseada em certificado será ativada automaticamente.
- Você pode adicionar um cluster por meio do Unified Manager CLI; 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 interface do usuário do Unified Manager. Você pode ver ["Comandos CLI do Unified Manager suportados"](#) para adicionar um cluster usando o Unified Manager CLI.
- Se a autenticação baseada em certificado estiver habilitada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurar em outro servidor do Unified Manager onde o nome do host ou endereço IP for alterado, o monitoramento do cluster poderá falhar. Para evitar a falha, edite e salve os detalhes do cluster. Para obter mais informações sobre a edição de detalhes do cluster, consulte ["Editando clusters"](#).
- No nível do cluster, a interface do 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 deverá 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 autoassinado ONTAP na interface de usuário do System Manager"](#).

- Uma única instância do Unified Manager pode suportar um número específico de nós. Se você precisar monitorar um ambiente que exceda a contagem de nós suportada, deverá instalar uma instância adicional do Unified Manager para monitorar alguns dos clusters. Para visualizar a lista de contagem de nós suportados, consulte o ["Guia de práticas recomendadas do Unified Manager"](#).

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de cluster**.

2. Na página Configuração do cluster, clique em **Adicionar**.
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 visualizar as informações do certificado sobre o cluster.
5. Clique em **Sim**.

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

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

Depois que todos os objetos de um novo cluster são descobertos, o Unified Manager começa a coletar dados históricos de desempenho dos 15 dias anteriores. Essas estatísticas são coletadas usando a funcionalidade de coleta de continuidade de dados. Este recurso fornece mais de duas semanas de informações de desempenho para um cluster imediatamente após ele 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.



- A coleta de 15 dias de dados de desempenho exige muito da CPU. A NetApp recomenda que você escalone 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 ausente.
- Quando você adiciona um cluster ONTAP com a versão 9.14.1 ou posterior, a comunicação ocorre por meio do recurso do agente de nuvem. O ONTAP cria automaticamente um usuário de conta de serviço interno com privilégios somente leitura (por exemplo, `clus-agent-xxxx`). O Unified Manager para de coletar dados desses clusters se o `clus-agent` o usuário é excluído.



Se você receber uma mensagem de erro informando que não é possível adicionar o cluster, verifique se os seguintes problemas existem:

- 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 estejam sincronizados usando NTP ou um serviço similar.
- Se o cluster atingir o número máximo de destinos de notificação EMS, o endereço do Unified Manager não poderá ser adicionado. Por padrão, apenas 20 destinos de notificação EMS podem ser definidos no cluster.

Informações relacionadas

["Adicionando usuários"](#)

["Visualizando a lista de clusters e detalhes"](#)

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

Editar clusters

Você pode modificar as configurações de um cluster existente, como o 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 de Administrador de Aplicativos ou a função de Administrador de Armazenamento.



A partir do Unified Manager 9.7, os clusters podem ser adicionados usando somente HTTPS.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de cluster**.
2. Na página **Configuração do 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 visualizar os detalhes do certificado para comunicação TLS mútua, com base na versão do ONTAP . Para mais informações sobre a versão ONTAP , consulte "[Certificados para comunicação TLS mútua](#)" . + Você pode visualizar os detalhes do certificado clicando em **Detalhes do certificado**. Se o certificado estiver 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 visualizar as informações do certificado sobre o cluster.
6. Clique em **Sim**.

Informações relacionadas

["Adicionando usuários"](#)

["Visualizando a lista de clusters e detalhes"](#)

Remover clusters

Você pode remover um cluster do Unified Manager usando a página Configuração do Cluster. Por exemplo, você pode remover um cluster se a descoberta do cluster falhar ou quando quiser desativar um sistema de armazenamento.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou a função de Administrador de 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 no cluster removido também não é registrada no cluster.

A remoção de um cluster também exclui todos os seus 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 de cluster**.
2. Na página Configuração do cluster, selecione o cluster que você deseja remover e clique em **Remover**.
3. Na caixa de diálogo da mensagem **Remover fonte de dados**, clique em **Remover** para confirmar a solicitação de remoção.

Informações relacionadas

["Adicionando usuários"](#)

["Visualizando a lista de clusters e detalhes"](#)

Redescubra clusters

Você pode redescobrir manualmente um cluster na página Configuração do Cluster para obter as informações mais recentes sobre a integridade, o status de monitoramento e o status de desempenho do cluster.

Você pode redescobrir manualmente um cluster quando quiser atualizá-lo (por exemplo, aumentando o tamanho de um agregado quando não houver espaço suficiente) e quiser que o Unified Manager descubra as alterações feitas.

Quando o Unified Manager é pareado com o OnCommand Workflow Automation (WFA), o pareamento aciona a reaquisição dos dados armazenados em cache pelo WFA.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de cluster**.
2. Na página **Configuração do cluster**, clique em **Redescobrir**.

O Unified Manager redescobre o cluster selecionado e exibe o status mais recente de integridade e desempenho.

Informações relacionadas

["Visualizando a lista de clusters e detalhes"](#)

Monitorar a infraestrutura virtual VMware

O Active IQ Unified Manager fornece visibilidade das máquinas virtuais (VMs) na sua infraestrutura virtual e permite monitorar e solucionar problemas de armazenamento e desempenho no seu ambiente virtual. Você pode usar esse recurso para determinar quaisquer problemas de latência no seu ambiente de armazenamento ou quando houver um evento de desempenho relatado no seu vCenter Server.

Uma implantação típica de infraestrutura virtual no ONTAP tem vários componentes distribuídos entre camadas de computação, rede e armazenamento. Qualquer atraso de desempenho em um aplicativo de VM pode ocorrer devido a uma combinação de latências enfrentadas pelos vários componentes nas respectivas camadas. Esse recurso é útil para administradores de armazenamento e 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 vCenter da seção VMware. A visualização rápida 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 visualizar os armazenamentos de dados no vCenter Server.

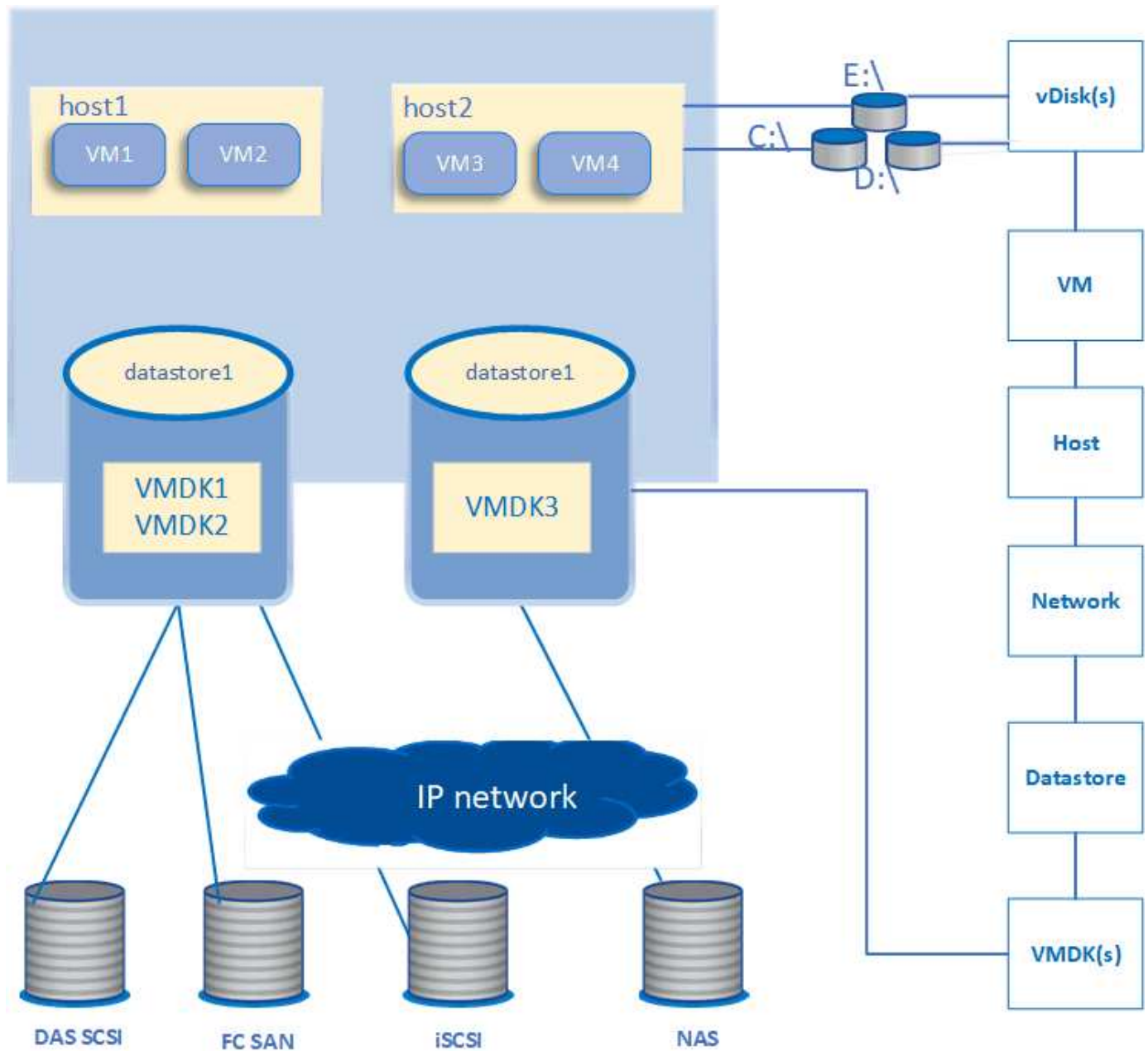
O Unified Manager apresenta o subsistema subjacente de um ambiente virtual em uma visão topológica para determinar se ocorreu um problema de latência no nó de computação, na rede ou no armazenamento. A exibição também destaca o objeto específico que causa o atraso no desempenho para tomar medidas corretivas e abordar o problema subjacente.

Uma infraestrutura virtual implantada no armazenamento ONTAP inclui os seguintes objetos:

- vCenter Server: um plano de controle centralizado para gerenciar VMs VMware, hosts ESXi e todos os componentes relacionados em um ambiente virtual. Para obter mais informações sobre o vCenter Server, consulte a documentação do VMware.
- Host: Um sistema físico ou virtual que executa o ESXi, o software de virtualização da VMware, e hospeda a VM.
- Armazenamento de dados: os armazenamentos de dados são objetos de armazenamento virtual conectados aos hosts ESXi. Os datastores são entidades de armazenamento gerenciáveis do ONTAP, como LUNs ou volumes, usados 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. Os armazenamentos de dados fora do ONTAP mapeados para o vCenter Server não são suportados nem exibidos no Unified Manager.
- VM: Uma máquina virtual VMware.
- Discos virtuais: Os discos virtuais em armazenamentos de dados 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 armazenamento de dados que fornece espaço de armazenamento para discos virtuais. Para cada disco virtual, há um VMDK correspondente.

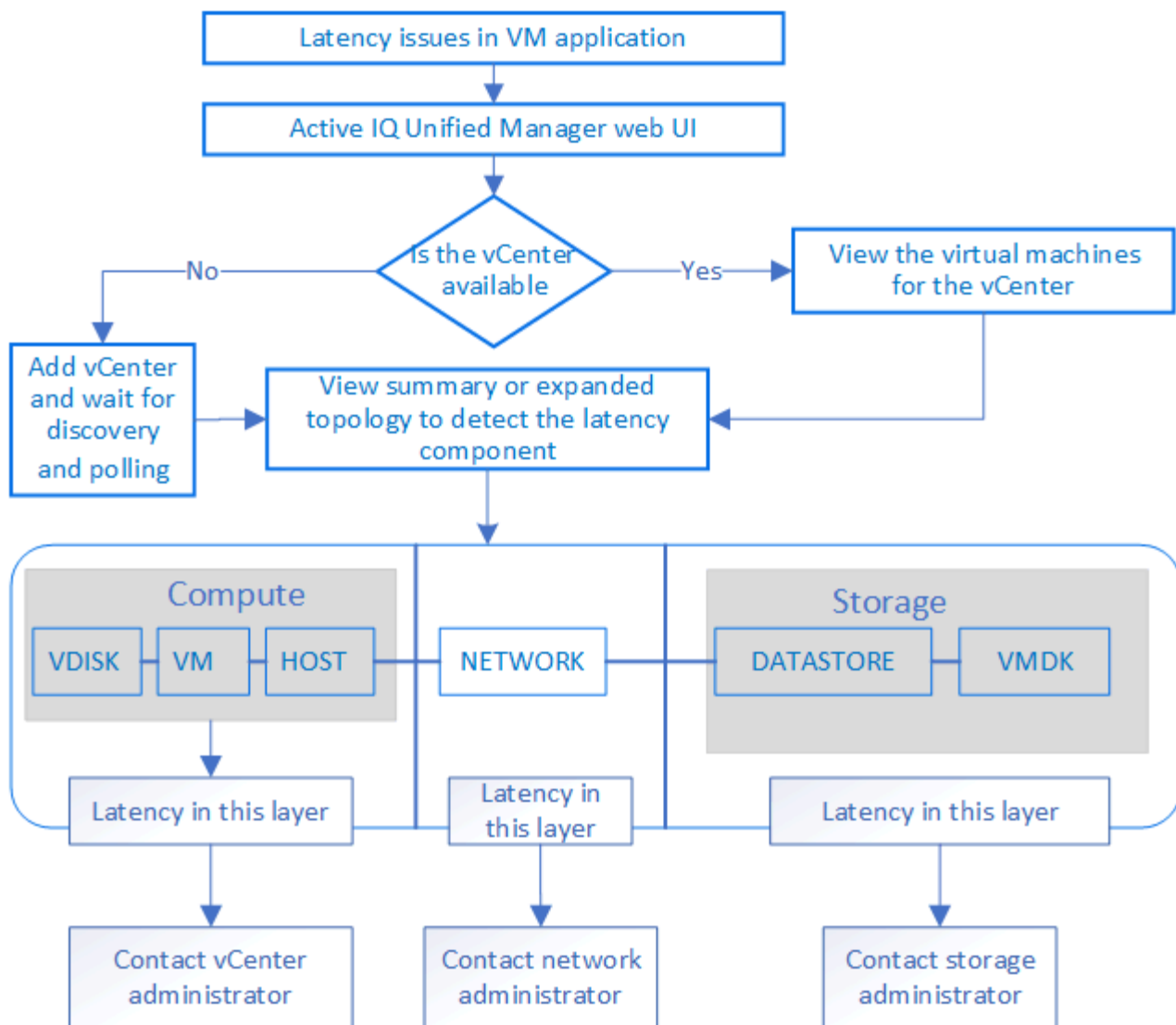
Esses objetos são representados em uma exibição de topologia de VM.

Virtualização VMware no ONTAP



Fluxo de trabalho do usuário

O diagrama a seguir exibe um caso de uso típico do uso da visualização de topologia de VM:



O que não é suportado

- Os armazenamentos de dados que estão fora do ONTAP e são mapeados para instâncias do vCenter Server não são suportados no Unified Manager. Nenhuma VM com discos virtuais nesses armazenamentos de dados é suportada.
- Um armazenamento de dados que abrange vários LUNs não é suportado.
- Os armazenamentos de dados que usam tradução de endereço de rede (NAT) para mapeamento de dados LIF (ponto de extremidade de acesso) não são suportados.
- Não há suporte para exportar volumes ou LUNs como armazenamentos de dados em clusters diferentes com os mesmos endereços IP em uma configuração de vários LIFs, pois o Unified Manager não consegue identificar qual armazenamento de dados pertence a qual cluster.

Exemplo: Suponha que o cluster A tenha o armazenamento de dados A. O armazenamento de dados A é exportado via LIF de dados com o mesmo endereço IP xxxx e a VM A é criada neste armazenamento de dados. Da mesma forma, o cluster B tem o armazenamento de dados B. O armazenamento de dados B é exportado via LIF de dados com o mesmo endereço IP xxxx e a VM B é criada no armazenamento de dados B. O UM não conseguirá mapear o armazenamento de dados A para a topologia da VM A para o volume/LUN ONTAP correspondente nem mapear a VM B.

- Somente volumes NAS e SAN (iSCSI e FCP para VMFS) são suportados como armazenamentos de

dados; volumes virtuais (vVols) não são suportados.

- Somente discos virtuais iSCSI são suportados. Discos virtuais dos tipos NVMe e SATA não são suportados.
- As visualizações não permitem gerar relatórios para analisar o desempenho dos vários componentes.
- Para a configuração de recuperação de desastres (DR) da máquina virtual de armazenamento (VM de armazenamento) que é suportada apenas para infraestrutura virtual no Unified Manager, a configuração precisa ser alterada manualmente no vCenter Server para apontar para os LUNs ativos em cenários de alternância e retorno. Sem uma intervenção manual, seus armazenamentos de dados se tornam inacessíveis.

Visualizar e adicionar o 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 servidores vCenter, verifique o seguinte:

- Você conhece os nomes do vCenter Server.
- Você sabe 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 para o nível de estatísticas de *Level 3* , 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 salvamento 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 do 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 armazenamento de dados ao vCenter Server, você pode usar o endereço IP do host ou o nome de domínio totalmente qualificado (FQDN). Caso você esteja adicionando FQDN, certifique-se de que o nome de domínio possa ser resolvido pelo servidor do Unified Manager. Por exemplo, para uma instalação Linux, certifique-se de que o nome de domínio seja adicionado no `/etc/resolv.conf` arquivo.
- O horário atual do vCenter Server está sincronizado 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 pesquisa 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 ONTAP , detalhes do armazenamento de

dados e número de VMs hospedadas. Ele também coleta as métricas de desempenho dos componentes.

Passos

1. Vá para **VMWARE > vCenter** e verifique se o seu vCenter Server está disponível na lista.



Se o seu vCenter Server não estiver disponível, você deverá adicioná-lo.

- a. Clique em **Adicionar**.
- b. Adicione o endereço IP correto para o vCenter Server e certifique-se de que o dispositivo esteja acessível.
- c. Adicione o nome de usuário e a senha do administrador ou usuário root com acesso somente leitura ao vCenter Server.
- d. Adicione o número da porta personalizada se estiver usando qualquer porta diferente da padrão 443.
- e. Clique em **Salvar**.

Após a descoberta bem-sucedida, um certificado de servidor será exibido para você aceitar.

Quando você aceita o certificado, o vCenter Server é adicionado à lista de vCenter Servers disponíveis. Adicionar o dispositivo não resulta na coleta de dados para as VMs associadas, e a coleta ocorre nos intervalos agendados.

2. Se o seu vCenter Server estiver disponível na página **vCenters**, verifique seu status passando o mouse sobre o campo **Status** para exibir se o seu vCenter Server está funcionando conforme o esperado ou se há um aviso ou erro.



Adicionar o vCenter Server permite que você visualize os seguintes status. No entanto, os dados de desempenho e latência das VMs correspondentes podem levar até uma hora após a adição do 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 qualquer erro interno, como exceção, falha na coleta de dados de configuração ou inacessibilidade do vCenter Server). Você pode clicar no ícone de exibição da coluna **(Mostrar/Ocultar)** para visualizar a mensagem de 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**.

Começa a coleta de dados do vCenter Server

O vCenter Server coleta amostras de dados de desempenho de 20 segundos em tempo real e as acumula em amostras de 5 minutos. O cronograma para coleta de dados de desempenho do Unified Manager é baseado nas configurações padrão do vCenter Server. O Unified Manager processa as amostras de 5 minutos obtidas do vCenter Server e calcula uma média horária de IOPS e latência para discos virtuais, VMs e hosts. Para armazenamentos de dados, o Unified Manager calcula uma média horária de IOPS e latência de amostras obtidas do ONTAP. Esses valores estão disponíveis no topo da hora. As métricas de desempenho não ficam disponíveis imediatamente após a adição do vCenter Server e só ficam disponíveis quando a próxima hora

começa. A pesquisa de dados de desempenho começa ao concluir um ciclo de coleta de dados de configuração.

Para pesquisar dados de configuração do vCenter Server, o Unified Manager segue o mesmo cronograma usado para coletar dados de configuração do cluster. Para obter informações sobre a configuração do vCenter Server e o cronograma de coleta de dados de desempenho, consulte "Configuração do cluster e atividade de coleta de dados de desempenho".

Informações relacionadas

["Configuração de cluster e atividade de coleta de dados de desempenho"](#)

Remover o vCenter Server

Você pode remover os 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 ele não for mais necessário.

A remoção de um vCenter Server também exclui todas as máquinas virtuais (VMs) hospedadas naquele vCenter e seus dados de configuração. Após a remoção do vCenter Server, 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 os servidores vCenter, verifique o seguinte:

- Você tem a função de Administrador de Aplicativos ou a função de Administrador de Armazenamento.
- Você deve estar ciente dos nomes do vCenter Server e dos respectivos endereços IP associados a eles.

Passos

1. No painel de navegação esquerdo, clique em **VMWARE>vCenter**.
2. Na página vCenters, selecione o vCenter Server que você deseja remover e clique em **Remover**.
3. Na caixa de diálogo da mensagem **Remover vCenter**, clique em **OK** para confirmar a solicitação de remoção.

Monitorar máquinas virtuais

Para qualquer problema de latência nos aplicativos da máquina virtual (VM), pode ser necessário monitorar as VMs para analisar e solucionar a causa. As VMs ficam disponíveis quando o vCenter Server e os clusters ONTAP que hospedam o armazenamento da 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 da rede, IOPS e latência da VM, armazenamento de dados e host são exibidas. Para uma VM que oferece suporte a vários armazenamentos de dados, a grade mostra as métricas do armazenamento de dados com a pior latência, com um ícone de asterisco (*) indicando armazenamentos de dados adicionais. Se você clicar no ícone, as métricas do armazenamento de dados adicional serão exibidas. Algumas dessas colunas não estão disponíveis para classificação e filtragem.



Para visualizar uma VM e seus detalhes, a descoberta (sondagem ou coleta de métricas) do cluster ONTAP deve ser concluída. Se o cluster for removido do Unified Manager, a VM não estará mais disponível após o próximo ciclo de descoberta.

Nesta 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 armazenamento de dados conectado a ela. A visualização da topologia exibe os componentes subjacentes em suas camadas específicas, na seguinte ordem: **Disco Virtual > VM > Host > Rede > Armazenamento de Dados > VMDK**.

Você pode determinar o caminho de E/S e as latências no nível do componente a partir de um aspecto topológico e identificar se o armazenamento é a causa do problema de desempenho. A exibição resumida da topologia exibe o caminho de E/S e destaca o componente que tem problemas de IOPS e latência para que você decida as etapas de solução de problemas. Você também pode ter uma visão expandida da topologia que descreve 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.

Ver topologia resumida

Para determinar problemas de desempenho visualizando as VMs em uma topologia resumida:

1. Vá para **VMWARE > Máquinas Virtuais**.
2. Procure sua VM digitando seu nome na caixa de pesquisa. Você também pode filtrar os resultados da sua pesquisa com base em critérios específicos clicando no botão **Filtrar**. No entanto, se você não conseguir encontrar sua VM, certifique-se de que o vCenter Server correspondente tenha sido adicionado e descoberto.



Os servidores vCenter permitem caracteres especiais (como %, &, *, \$, #, @, !, \, /, :, *, ?, ", <, >, |, ;, ') nos nomes de entidades do vSphere, como VM, cluster, armazenamento de dados, pasta ou arquivo. O VMware vCenter Server e o ESX/ESXi Server não escapam 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 chamada como %\$VC_AIQUM_clone_191124% no vCenter Server é exibido como %25\$VC_AIQUM_clone_191124%25 no Unified Manager. Você deve anotar esse problema ao consultar uma VM cujo nome contém caracteres especiais.

3. Verifique o status da VM. Os status da VM são recuperados do vCenter Server. Os seguintes status estão disponíveis. Para obter mais informações sobre esses status, consulte a documentação do VMware.
 - Normal
 - Aviso
 - Alerta
 - Não monitorado
 - Desconhecido
4. Clique na seta para baixo ao lado da VM para ver a visão resumida 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, esta exibição mostrará o disco virtual que tem a pior latência entre todos os discos virtuais.
5. Para analisar a latência e a taxa de transferência do armazenamento de dados ao longo de um período de tempo, clique no botão **Analisador de Carga de Trabalho** na parte superior do ícone do objeto do armazenamento de dados. Acesse a página Análise de Carga de Trabalho, onde você pode selecionar um intervalo de tempo e visualizar os gráficos de desempenho do armazenamento de dados. Para obter mais

informações sobre o analisador de carga de trabalho, consulte *Solução de problemas de cargas de trabalho usando o analisador de carga de trabalho*.

Ver topologia expandida

Você pode detalhar cada componente separadamente visualizando a topologia expandida da VM.

Passos

1. Na visualização resumida da topologia, 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 armazenamento de dados ou VMDK, o nó com pior latência será destacado 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 seu mapeamento destacado para o respectivo VMDK. Em caso de atraso no 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 cargas de trabalho usando o Workload Analyzer"](#)

Visualizar infraestrutura virtual em uma configuração de recuperação de desastres

Você pode visualizar as métricas de configuração e desempenho dos datastores hospedados em uma configuração do MetroCluster ou na configuração de recuperação de desastres da máquina virtual de armazenamento (VM de armazenamento) (SVM DR).

No Unified Manager, você pode visualizar os volumes NAS ou LUNs em uma configuração do MetroCluster que estão anexados como armazenamentos de dados no vCenter Server. Os armazenamentos de dados hospedados em uma configuração MetroCluster são representados na mesma visualização topológica de um armazenamento de dados em um ambiente padrão.

Você também pode visualizar os volumes NAS ou LUNs em uma configuração de recuperação de desastres de VM de armazenamento que são mapeados para os armazenamentos de dados no vCenter Server.

Exibir armazenamentos de dados na configuração do MetroCluster

Observe os seguintes pré-requisitos antes de visualizar armazenamentos de dados em uma configuração do MetroCluster :

- Em um evento de comutação e retorno, a descoberta dos clusters primário e secundário do par HA e dos servidores vCenter deve ser concluída.
- Os clusters primário e secundário do par HA e os vCenter Servers devem 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 ONTAP 9"](#)

Siga estas etapas para visualizar os armazenamentos de dados:

1. Na página **VMWARE > Máquinas Virtuais**, clique na VM que hospeda o armazenamento de dados. Clique no **Workload Analyzer** ou no link do objeto de armazenamento de dados. No cenário padrão, quando o site principal que hospeda o volume ou LUN está funcionando conforme o esperado, você pode ver os detalhes do cluster vServer do site principal.
2. Em caso de desastre e uma troca consecutiva para o site secundário, o link do armazenamento de dados aponta para as métricas de desempenho do volume ou LUN no cluster secundário. Isso se reflete após a conclusão do próximo ciclo de clusters e da descoberta (aquisição) do vServer.
3. Após uma troca bem-sucedida, o link do armazenamento de dados reflete novamente as métricas de desempenho do volume ou LUN no cluster primário. Isso se reflete após a conclusão do próximo ciclo de clusters e da descoberta do vServer.

Exibir datastores na configuração de recuperação de desastres da VM de armazenamento

Observe os seguintes pré-requisitos antes de visualizar os armazenamentos de dados em uma configuração de recuperação de desastres de VM de armazenamento:

- Em um evento de comutação e retorno, a descoberta dos clusters primário e secundário do par HA e dos servidores vCenter deve ser concluída.
- Tanto o cluster de origem quanto o de destino e os pares de VM de armazenamento 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 ativar a VM de armazenamento secundário, verificar os LIFs e rotas de dados, estabelecer conexões perdidas no vCenter Server e iniciar as VMs.

Para retornar ao 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 ativar a VM de armazenamento secundário e verificar os LIFs e rotas de dados. Se os IPs de destino do iSCSI forem diferentes dos LIFs primários, eles precisarão ser adicionados manualmente. Os novos LUNs devem estar disponíveis como dispositivos no adaptador iSCSI do adaptador de armazenamento do host. Depois disso, novos datastores VMFS com os novos LUNs devem ser criados e as VMs antigas registradas com novos nomes. As VMs devem estar ativas e em execução.

Em caso de recuperação, os dados entre os volumes devem ser sincronizados. Novos datastores VMFS devem ser criados novamente usando os 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 ONTAP 9"](#)

Siga estas etapas para visualizar os armazenamentos de dados:

1. Na página **VMWARE > Máquinas Virtuais**, clique no inventário de VM que hospeda o armazenamento de dados. Clique no link do objeto do armazenamento de dados. No cenário padrão, você pode ver os dados de desempenho dos volumes e LUNs na VM de armazenamento primário.

2. Em caso de desastre e uma troca consecutiva para a VM de armazenamento secundário, o link do armazenamento de dados aponta para as métricas de desempenho do volume ou LUN na VM de armazenamento secundário. Isso se reflete após a conclusão do próximo ciclo de clusters e da descoberta (aquisição) do vServer.
3. Após uma troca bem-sucedida, o link do armazenamento de dados reflete novamente as métricas de desempenho do volume ou LUN na VM de armazenamento primário. Isso se reflete após a conclusão do próximo ciclo de clusters e da descoberta do vServer.

Cenários não suportados

- Para uma configuração do MetroCluster, observe as seguintes limitações:
 - Aglomerados somente no NORMAL e SWITCHOVER estados são assumidos. Outros estados, como PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK, e NOT_REACHABLE não são suportados.
 - A menos que a Comutação Automática (ASO) esteja habilitada, se o cluster primário ficar inativo, o cluster secundário não poderá ser descoberto e a topologia continuará apontando para o volume ou LUN no cluster primário.
- Para uma configuração de recuperação de desastres de VM de armazenamento, observe a seguinte limitação:
 - Uma configuração com o Site Recovery Manager (SRM) ou o Storage Replication Adapter (SRA) habilitado para um ambiente de armazenamento SAN não é suportada.

Provisionar e gerenciar cargas de trabalho

O recurso de gerenciamento ativo do Active IQ Unified Manager fornece níveis de serviço de desempenho, políticas de eficiência de armazenamento e APIs de provedores de armazenamento para provisionamento, monitoramento e gerenciamento de cargas de trabalho de armazenamento em um data center.



O Unified Manager fornece essa funcionalidade por padrão. Você pode desativá-lo em **Gerenciamento de armazenamento > Configurações de recursos** se não planeja usar essa funcionalidade.

Quando ativado, você pode provisionar cargas de trabalho nos clusters ONTAP gerenciados pela sua instância do Unified Manager. Você também pode atribuir políticas, como Níveis de Serviço de Desempenho e Políticas de Eficiência de Armazenamento nas cargas de trabalho e gerenciar seu ambiente de armazenamento com base nessas políticas.

Este recurso habilita as seguintes funções:

- Descoberta automática de cargas de trabalho de armazenamento nos clusters adicionados, permitindo fácil avaliação e implantação da carga de trabalho de armazenamento
- Provisionamento de cargas de trabalho NAS com suporte aos protocolos NFS e CIFS
- Provisionamento de cargas de trabalho SAN com suporte aos protocolos iSCSI e FCP
- Suporte para protocolos NFS e CIFS no mesmo compartilhamento de arquivos
- Gestão de Níveis de Serviço de Desempenho e Políticas de Eficiência de Armazenamento
- Atribuição de níveis de serviço de desempenho e políticas de eficiência de armazenamento para cargas de trabalho de armazenamento

As opções **Provisionamento**, **Armazenamento** > **Cargas de trabalho** e **Políticas** no painel esquerdo da interface do usuário permitem que você modifique várias configurações.

Você pode executar as seguintes funções usando estas opções:

- Visualize as cargas de trabalho de armazenamento na página **Armazenamento** > **Cargas de trabalho**
- Crie cargas de trabalho de armazenamento na página Provisionar carga de trabalho
- Crie e gerencie níveis de serviço de desempenho a partir de políticas
- Crie e gerencie políticas de eficiência de armazenamento a partir de políticas
- Atribuir políticas a cargas de trabalho de armazenamento na página Cargas de trabalho

Informações relacionadas

["Gerenciamento de armazenamento baseado em políticas"](#)

Visão geral das cargas de trabalho

Uma carga de trabalho representa as operações de entrada/saída (E/S) de um objeto de armazenamento, como um volume ou LUN. A maneira como o armazenamento é provisionado é baseada nos requisitos de carga de trabalho esperados. As estatísticas de carga de trabalho são rastreadas pelo Active IQ Unified Manager somente depois que há tráfego de e para o objeto de armazenamento. Por exemplo, os valores de IOPS e latência da carga de trabalho ficam disponíveis depois que os usuários começam a usar um banco de dados ou aplicativo de e-mail.

A página Cargas de trabalho exibe um resumo das cargas de trabalho de armazenamento dos clusters ONTAP gerenciados pelo Unified Manager. Ele fornece informações cumulativas e rápidas sobre as cargas de trabalho de armazenamento que estão em conformidade com o Nível de Serviço de Desempenho, bem como as cargas de trabalho de armazenamento não conformes. Ele também permite que você avalie a capacidade e o desempenho (IOPS) total, disponível e utilizado dos clusters em seu data center.



É recomendável que você avalie o número de cargas de trabalho de armazenamento que não estão em conformidade, não estão disponíveis ou não são gerenciadas por nenhum Nível de Serviço de Desempenho e tome as ações necessárias para garantir sua conformidade, uso de capacidade e IOPS.

A página Cargas de trabalho tem as duas seções a seguir:

- Visão geral das cargas de trabalho: fornece uma visão geral do número de cargas de trabalho de armazenamento nos clusters ONTAP gerenciados pelo Unified Manager.
- Visão geral do data center: fornece uma visão geral da capacidade e do IOPS das cargas de trabalho de armazenamento no data center. Os dados relevantes são exibidos no nível do centro de dados e para cada indivíduo.

Seção de visão geral das cargas de trabalho

A seção de visão geral das cargas de trabalho fornece informações cumulativas e rápidas sobre as cargas de trabalho de armazenamento. O status das cargas de trabalho de armazenamento é exibido com base nos Níveis de Serviço de Desempenho atribuídos e não atribuídos.

- **Atribuído:** Os seguintes status são relatados para cargas de trabalho de armazenamento nas quais os Níveis de Serviço de Desempenho foram atribuídos:
 - **Em conformidade:** O desempenho das cargas de trabalho de armazenamento é baseado nos Níveis de Serviço de Desempenho atribuídos a elas. Se as cargas de trabalho de armazenamento estiverem dentro da latência limite definida nos Níveis de Serviço de Desempenho associados, elas serão marcadas como “em conformidade”. As cargas de trabalho em conformidade são marcadas em azul.
 - **Não conforme:** Durante o monitoramento de desempenho, as cargas de trabalho de armazenamento são marcadas como “não conformes” se a latência das cargas de trabalho de armazenamento exceder a latência limite definida no Nível de Serviço de Desempenho associado. As cargas de trabalho não conformes são marcadas em laranja.
 - **Indisponível:** as cargas de trabalho de armazenamento são marcadas como “indisponíveis” se estiverem offline ou se o cluster correspondente estiver inacessível. As cargas de trabalho indisponíveis são marcadas em vermelho.
- **Não atribuído:** cargas de trabalho de armazenamento que não têm 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 da carga de trabalho 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 armazenamento disponíveis:

- Conforme cada tipo de Nível de Serviço de Desempenho
- Para o 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 utilizada, e o IOPS para todos os clusters no data center. Ao usar esses dados, você deve gerenciar a capacidade e o IOPS das cargas de trabalho de armazenamento. A seção também exibe as seguintes informações para as cargas de trabalho de armazenamento em todos os clusters:

- A capacidade total, disponível e usada para todos os clusters em seu data center
- O IOPS total, disponível e usado para todos os clusters no seu data center
- A capacidade disponível e utilizada com base em cada Nível de Serviço de Desempenho
- Os IOPS disponíveis e utilizados com base em cada Nível de Serviço de Desempenho
- O espaço total e IOPS usados pelas cargas de trabalho que não têm Nível de Serviço de Desempenho atribuído

Como a capacidade e o desempenho do data center são calculados com base nos níveis de serviço de desempenho

A capacidade utilizada e o IOPS são recuperados em termos da capacidade total utilizada e do desempenho de todas as cargas de trabalho de armazenamento nos clusters.

O IOPS disponível é calculado com base na latência esperada e nos Níveis de Serviço de Desempenho recomendados nos nós. Inclui o IOPS disponível para todos os Níveis de Serviço de Desempenho 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. Inclui a capacidade disponível para todos os Níveis de Serviço de Desempenho cuja latência esperada é menor ou igual à sua própria latência esperada.

Exibir cargas de trabalho

Quando você adiciona clusters ao Unified Manager, as cargas de trabalho de armazenamento em cada cluster são descobertas automaticamente e exibidas na página Cargas de trabalho.

O Unified Manager começa a analisar as cargas de trabalho para recomendação (PSLs recomendados) somente depois que as operações de E/S começam nas cargas de trabalho de armazenamento.

Os volumes do FlexGroup e seus constituintes são excluídos.

Visão geral das cargas de trabalho

A página Visão geral das cargas de trabalho exibe a visão geral das cargas de trabalho no data center e a visão geral do 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 atribuídos a elas. A divisão 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 visualizar o número de cargas de trabalho que não estão em conformidade com a recomendação do sistema e atribuir os PSLs recomendados pelo sistema a elas clicando no botão **Atribuir PSLs recomendados pelo sistema**.
- Painel **Visão geral do data center**: exibe o espaço disponível e usado (TiB) e o desempenho (IOPS) do data center. Uma análise do espaço disponível e usado (TiB) e do desempenho (IOPS) de todas as cargas de trabalho em cada PSL também é exibida.

Visualização de todas as cargas de trabalho

A página **Armazenamento > Cargas de trabalho > Todas as cargas de trabalho** lista as cargas de trabalho de armazenamento associadas aos clusters ONTAP gerenciados pelo Unified Manager.

Para as cargas de trabalho de armazenamento recém-descobertas nas quais não houve operações de E/S, o status é “Aguardando E/S”. Depois que as operações de E/S começam nas cargas de trabalho de armazenamento, o Unified Manager inicia a análise e o status da carga de trabalho muda para “Aprendendo...”. Após a conclusão da análise (dentro de 24 horas do início das operações de E/S), os PSLs recomendados são exibidos para as cargas de trabalho de armazenamento.

A página também permite que você atribua Políticas de Eficiência de Armazenamento (SEPs) e Níveis de Serviço de Desempenho (PSLs) a cargas de trabalho de armazenamento. Você pode executar várias tarefas:

- Adicionar ou provisionar cargas de trabalho de armazenamento
- Visualizar e filtrar a lista de cargas de trabalho
- Atribuir PSLs a cargas de trabalho de armazenamento
- Avalie os PSLs recomendados pelo sistema e atribua-os às cargas de trabalho
- Atribuir SEPs a cargas de trabalho de armazenamento

Adicionar ou provisionar cargas de trabalho de armazenamento

Você pode adicionar ou provisionar cargas de trabalho de armazenamento para LUNs compatíveis (compatíveis com os protocolos iSCSI e FCP), compartilhamentos de arquivos NFS e compartilhamentos SMB.

Passos

1. Clique em **Armazenamento > Cargas de trabalho > Todas as cargas de trabalho > Criar**.
2. Crie cargas de trabalho. Para obter informações, consulte ["Provisionamento e gerenciamento de cargas de trabalho"](#).

Visualização e filtragem de cargas de trabalho

Na tela Todas as cargas de trabalho, você pode visualizar todas as cargas de trabalho no seu data center ou pesquisar cargas de trabalho de armazenamento específicas com base em seus PSLs ou nomes. Você pode usar o ícone de filtro para inserir condições específicas para sua pesquisa. Você pode pesquisar por diferentes condições de filtro, como pelo cluster do host ou pela VM de armazenamento. A opção **Capacidade Total** permite filtrar pela capacidade total das cargas de trabalho (por MB). Entretanto, neste caso, o número de cargas de trabalho retornadas pode variar, porque a capacidade total é comparada em nível de byte.

Para cada carga de trabalho, informações como o cluster do host e a VM de armazenamento são exibidas, juntamente com o PSL e o SEP atribuídos.

A página também permite que você visualize os detalhes de desempenho de uma carga de trabalho. Você pode visualizar informações detalhadas sobre IOPS, capacidade e latência da carga de trabalho clicando no botão **Escolher / Ordenar colunas** e selecionando colunas específicas para visualizar. A coluna Exibição de desempenho exibe o IOPS médio e máximo para uma carga de trabalho, e você pode clicar no ícone do analisador de carga de trabalho para visualizar a análise detalhada do IOPS.

Analisando critérios de desempenho e capacidade para uma carga de trabalho

O botão **Analisar carga de trabalho** no pop-up **Análise de IOPS** leva você para a página Análise de carga de trabalho, onde você pode selecionar um intervalo de tempo e visualizar 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, consulte ["Solução de problemas de cargas de trabalho usando o analisador de carga de trabalho"](#).

Você pode visualizar informações de desempenho sobre uma carga de trabalho para ajudar na solução de problemas clicando no ícone do gráfico de barras na coluna **Visualização de desempenho**. Para visualizar gráficos de desempenho e capacidade na página Análise de carga de trabalho para analisar o objeto, clique no botão **Analisar carga de trabalho**.

Para mais informações, consulte ["Quais dados o analisador de carga de trabalho exibe"](#).

Atribuir políticas a cargas de trabalho

Você pode atribuir Políticas de Eficiência de Armazenamento (SEPs) e Níveis de Serviço de Desempenho (PSLs) a cargas de trabalho de armazenamento na página Todas as Cargas de Trabalho usando as diferentes opções de navegação.

Atribuir 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 depois clique em **Editar**.

Os campos **Nível de serviço de desempenho atribuído** e **Política de eficiência de armazenamento** estão habilitados.

3. Selecione o PSL ou SEP desejado, 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.

Atribuir políticas a várias cargas de trabalho de armazenamento

Você pode atribuir um PSL ou um SEP a várias cargas de trabalho de armazenamento juntas. 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 no seu data center.
2. Clique em **Mais ações**.
3. Para atribuir um PSL, selecione **Atribuir Nível de Serviço de Desempenho**. Para atribuir um SEP, selecione **Atribuir política de eficiência de armazenamento**. Um pop-up será exibido para você selecionar a política.
4. Selecione a política apropriada e clique em **Aplicar**. 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 visualizar o status de conclusão. Se você estiver aplicando um PSL em várias cargas de trabalho, não poderá acionar outra solicitação quando o trabalho anterior de atribuição em massa estiver em execução.

Atribuir PSLs recomendados pelo sistema às cargas de trabalho

Você pode atribuir PSLs recomendados pelo sistema às cargas de trabalho de armazenamento em um data center que não têm PSLs atribuídos ou que os PSLs atribuídos não correspondem à recomendação do sistema. Para usar esta funcionalidade, clique no botão **Atribuir PSLs recomendados pelo sistema**. Você não precisa 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 nenhum PSL disponível. Cargas de trabalho de armazenamento com `Waiting for I/O` e os status de Aprendizagem 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 Desempenho Recomendado ao Sistema' não é adaptável a uma carga de trabalho altamente variável"](#)

Provisionar volumes de compartilhamento de arquivos

Você pode criar volumes de compartilhamento de arquivos que suportam protocolos CIFS/SMB e NFS em um cluster existente e em uma Máquina Virtual de Armazenamento (VM de armazenamento) na página Provisionar Carga de Trabalho.

Antes de começar

- A VM de armazenamento deve ter espaço para provisionar o volume de compartilhamento de arquivos.
- Um ou ambos os serviços SMB e NFS devem estar habilitados na sua VM de armazenamento.
- 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 você começar a criar a carga de trabalho.

Passos

1. Na página **Provisionar carga de trabalho**, adicione o nome da carga de trabalho que você deseja criar e selecione o cluster na lista disponível.
2. Com base no cluster selecionado, o campo **VM DE ARMAZENAMENTO** filtra as VMs de armazenamento disponíveis para esse cluster. Selecione a VM de armazenamento necessária na lista.

Com base nos serviços SMB e NFS suportados na VM de armazenamento, a opção NAS é habilitada na seção Informações do Host.

3. Na seção Armazenamento e Otimização, atribua a capacidade de armazenamento e o PSL e, opcionalmente, um SEP para a carga de trabalho.

As especificações para o SEP são atribuídas ao LUN e as definições para o PSL são aplicadas à carga de trabalho quando ela é criada.

4. Marque a caixa de seleção **Aplicar limites de desempenho** se quiser aplicar o PSL que você atribuiu à carga de trabalho.

Atribuir um PSL a uma carga de trabalho garante que o agregado no qual a carga de trabalho é criada possa dar suporte aos objetivos de desempenho e capacidade definidos na respectiva política. Por exemplo, se uma carga de trabalho for atribuída ao PSL "Desempenho Extremo", o agregado no qual a carga de trabalho será provisionada deverá ter a capacidade de dar suporte aos objetivos de desempenho e capacidade da política "Desempenho Extremo", como armazenamento SSD.



A menos que você marque esta 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 você não conseguir ver a opção **NAS** habilitada, verifique se a VM de armazenamento selecionada oferece suporte a SMB ou NFS, ou ambos.



Se sua VM de armazenamento estiver habilitada para serviços SMB e NFS, você poderá marcar as caixas de seleção **Compartilhar por NFS** e **Compartilhar por SMB** e criar um compartilhamento de arquivos que suporte os protocolos NFS e SMB. Se você quiser criar um compartilhamento SMB ou CIFS, marque apenas a caixa de seleção respectiva.

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, caso haja 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 políticas 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 atribua 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**.

A carga de trabalho é adicionada à lista de cargas de trabalho de armazenamento.

Provisionar LUNs

Você pode criar LUNs que suportam protocolos CIFS/SMB e NFS em um cluster existente e em uma Máquina Virtual de Armazenamento (VM de armazenamento) na página Provisionar Carga de Trabalho.

Antes de começar

- A VM de armazenamento deve ter espaço para provisionar o LUN.
- Tanto o iSCSI quanto o FCP devem estar habilitados na VM de armazenamento 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 você começar a criar a carga de trabalho.

Passos

1. Na página **Provisionar carga de trabalho**, adicione o nome da carga de trabalho que você deseja criar e selecione o cluster na lista disponível.

Com base no cluster selecionado, o campo **VM DE ARMAZENAMENTO** 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 é habilitada na seção Informações do Host.

3. Na seção **Armazenamento e Otimização**, atribua a capacidade de armazenamento e o PSL e, opcionalmente, o SEP para a carga de trabalho.

As especificações para o SEP são atribuídas ao LUN e as definições para o PSL são aplicadas à carga de trabalho quando ela é criada.

4. Marque a caixa de seleção **Aplicar limites de desempenho** se desejar aplicar o PSL atribuído à carga de trabalho.

Atribuir um PSL a uma carga de trabalho garante que o agregado no qual a carga de trabalho é criada possa dar suporte aos objetivos de desempenho e capacidade definidos na respectiva política. Por exemplo, se uma carga de trabalho receber o PSL "Desempenho Extremo", o agregado no qual a carga de trabalho será provisionada deverá ter a capacidade de dar suporte aos objetivos de desempenho e capacidade da política "Desempenho Extremo", como armazenamento SSD.



A menos que você selecione esta caixa de seleção, o PSL não será aplicado à carga de trabalho e o status da carga de trabalho no painel aparecerá como `unassigned`.

5. Selecione a opção **SAN**. Se você não conseguir ver a opção **SAN** habilitada, verifique se a VM de armazenamento selecionada oferece suporte a iSCSI e FCP.
6. Selecione o sistema operacional host.
7. Especifique o mapeamento do host para controlar o acesso dos iniciadores ao LUN. Você pode atribuir grupos iniciadores existentes (igroups) ou definir e mapear novos igroups.



Se você criar um novo igroup durante o provisionamento do LUN, precisará aguardar até o próximo ciclo de descoberta (até 15 minutos) para usá-lo. Portanto, é recomendável que você use um igroup existente da lista de igroups disponíveis.

Se você quiser criar um novo igroup, selecione o botão **Criar um novo grupo iniciador** e insira as informações do igroup.

8. Clique em **Salvar**.

O LUN é adicionado à lista de cargas de trabalho de armazenamento.

Níveis de serviço de desempenho

Um Nível de Serviço de Desempenho (PSL) permite que você defina os objetivos de desempenho e armazenamento para uma carga de trabalho. Você pode atribuir um PSL a uma carga de trabalho ao criá-la inicialmente ou depois editando-a.

O gerenciamento e o monitoramento dos recursos de armazenamento são baseados em Objetivos de Nível de Serviço (SLOs). Os SLOs são definidos por acordos de nível de serviço baseados no desempenho e na capacidade exigidos. No Unified Manager, os SLOs referem-se às definições de PSL dos aplicativos que estão sendo executados no armazenamento NetApp. Os serviços de armazenamento são diferenciados com base no desempenho e na utilização dos recursos subjacentes. Um PSL é uma descrição dos objetivos do serviço de armazenamento. Um PSL permite que o provedor de armazenamento especifique os objetivos de desempenho e capacidade para a carga de trabalho. Quando você atribui um PSL a uma carga de trabalho, a carga de trabalho correspondente no ONTAP é gerenciada por seus objetivos de desempenho e capacidade. Cada PSL é governado por IOPs de pico, esperados e mínimos absolutos, além de latência esperada.

O Unified Manager tem os seguintes tipos de PSLs:

- **Definido pelo sistema:** O Unified Manager fornece algumas políticas predefinidas que não podem ser alteradas. Esses PSLs predefinidos são:
 - Desempenho extremo
 - Desempenho
 - Valor

Os PSLs de Desempenho Extremo, Desempenho e Valor são aplicáveis à maioria das cargas de trabalho de armazenamento comuns em um data center.

O Unified Manager também oferece três níveis de serviço de desempenho para aplicativos de banco de dados. São PSLs de altíssimo desempenho que suportam IOPS intermitentes e são apropriados para aplicativos de banco de dados com a maior demanda de taxa de transferência.

- Extremo para logs 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 às suas necessidades, você poderá criar novos PSLs para atender às suas necessidades. Para obter informações, consulte ["Criar e editar níveis de serviço de desempenho"](#).
- **Beyond Extreme:** Os PSLs Beyond Extreme são os PSLs recomendados pelo sistema, sugeridos para cargas de trabalho que exigem IOPs maiores que Extreme. As cargas de trabalho são analisadas internamente com base em seu IOPS, capacidade e latência, e um Beyond Extreme PSL é recomendado para cada uma dessas cargas de trabalho na tela **Armazenamento > Cargas de trabalho > Todas as cargas de trabalho**. Você pode aplicar os 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 que uma carga de trabalho tenha os IOPs de pico e esperados como 106345 e 37929 respectivamente, o Beyond Extreme PSL gerado para a carga de trabalho é denominado como `Beyond Extreme 106345 37929`. Embora esses PSLs sejam recomendados pelo sistema, quando você os atribui a cargas de trabalho, esses PSLs são rotulados como `User-defined` no tipo.

Gerencie cargas de trabalho atribuindo PSLs

Você pode acessar os PSLs na página **Políticas > Níveis de serviço de desempenho** e usando as APIs do provedor de armazenamento. Gerenciar cargas de trabalho de armazenamento atribuindo PSLs a elas é conveniente, pois você não precisa gerenciar as cargas de trabalho de armazenamento individualmente. Quaisquer modificações também podem ser gerenciadas reatribuindo outro PSL em vez de gerenciá-las individualmente. O Unified Manager ajuda você a atribuir PSLs em suas cargas de trabalho com base em avaliações e recomendações internas.

Para obter informações sobre como atribuir PSLs recomendados pelo sistema a cargas de trabalho, consulte ["Atribuir PSLs recomendados pelo sistema às cargas de trabalho"](#)

A página Níveis de serviço de desempenho lista as políticas de PSL disponíveis e permite que você as adicione, edite e exclua.



Não é possível modificar um PSL definido pelo sistema ou que esteja atualmente atribuído a uma carga de trabalho. Não é possível excluir um PSL atribuído a uma carga de trabalho ou se ele 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 pelo usuário.
IOPS/TB esperado	Número mínimo de IOPS que um aplicativo deve executar em um LUN ou compartilhamento de arquivos. IOPS esperado especifica o IOPS mínimo esperado alocado, com base no tamanho alocado do objeto de armazenamento.
Pico IOPS/TB	Número máximo de IOPS que um aplicativo pode executar em um LUN ou compartilhamento de arquivos. O pico de IOPS especifica o máximo possível de IOPS alocado, com base no tamanho alocado do objeto de armazenamento ou no tamanho usado do objeto de armazenamento. Os IOPS de pico são baseados em uma política de alocação. A política de alocação é espaço alocado ou espaço usado. Quando a política de alocação é definida como espaço alocado, o pico de IOPS é calculado com base no tamanho do objeto de armazenamento. Quando a política de alocação é definida como espaço usado, o pico de IOPS é calculado com base na quantidade de dados armazenados no objeto de armazenamento, levando em consideração a eficiência do armazenamento. Por padrão, a política de alocação é definida como espaço usado.

Campo	Descrição
IOPS mínimo absoluto	O IOPS mínimo absoluto é usado como uma substituição quando o IOPS esperado é menor que esse valor. Os valores padrão dos PSLs definidos pelo sistema são os seguintes: • Desempenho extremo: se IOPS esperado $\geq$ 6144/TB, então IOPS mínimo absoluto = 1000 • Desempenho: Se IOPS esperados $\geq$ 2048/TB e $<$ 6144/TB, então IOPS mínimo absoluto = 500 • Valor: Se IOPS esperado $\geq$ 128/TB e $<$ 2048/TB, então IOPS mínimo absoluto = 75 Os valores padrão dos PSLs do banco de dados definidos pelo sistema são os seguintes: • Extremo para logs de banco de dados: se IOPS esperado $\geq$ 22528, então IOPS mínimo absoluto = 4000 • Extremo para dados compartilhados de banco de dados: se IOPS esperado $\geq$ 16384, então IOPS mínimo absoluto = 2000 • Extremo para dados de banco de dados: se IOPS esperado $\geq$ 12288, então IOPS mínimo absoluto = 2000 O valor mais alto do IOPS mínimo absoluto para PSLs personalizados pode ser no máximo 75.000. O valor mais baixo é calculado da seguinte forma: $1000/\text{latência esperada}$
Latência esperada	Latência esperada para IOPS de armazenamento em milissegundos por operação (ms/op).
Capacidade	Capacidade total disponível e utilizada nos clusters.
Cargas de trabalho	Número de cargas de trabalho de armazenamento às quais o PSL foi atribuído.

Para obter informações sobre como o pico de IOPS e os IOPS esperados ajudam a alcançar um desempenho diferenciado consistente em clusters ONTAP , consulte o seguinte artigo da KB:https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["O que é Orçamento de Desempenho?"]

Eventos gerados para cargas de trabalho que violam o limite definido pelos PSLs

Observe que, se as cargas de trabalho excederem o valor de latência esperado em 30% do tempo durante a hora anterior, o Unified Manager gerará um dos seguintes eventos para notificá-lo sobre um possível problema de desempenho:

- Limite de latência do volume de carga de trabalho violado, conforme definido pela Política de nível de serviço de desempenho
- Limite de latência do LUN da carga de trabalho violado, conforme definido pela Política de nível de serviço de desempenho.

Talvez você queira analisar a carga de trabalho para ver o que pode estar causando os valores de latência mais altos.

Para 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 da carga de trabalho para identificar problemas de desempenho"](#)
- ["O que são eventos de performance"](#)

PSLs definidos pelo sistema

A tabela a seguir fornece informações sobre os PSLs definidos pelo sistema:

Nível de serviço de desempenho	Descrição e caso de uso	Latência esperada (ms/op)	IOPS de pico	IOPS esperado	IOPS mínimo absoluto
Desempenho extremo	Fornecer rendimento extremamente alto com latência muito baixa Ideal para aplicações sensíveis à latência	1	12288	6144	1000
Desempenho	Fornecer alto rendimento com baixa latência Ideal para bancos de dados e aplicativos virtualizados	2	4096	2048	500

Nível de serviço de desempenho	Descrição e caso de uso	Latência esperada (ms/op)	IOPS de pico	IOPS esperado	IOPS mínimo absoluto
Valor	Oferece alta capacidade de armazenamento e latência moderada Ideal para aplicações de alta capacidade, como e-mail, conteúdo da web, compartilhamentos de arquivos e destinos de backup	17	512	128	75
Extremo para logs de banco de dados	Fornece rendimento máximo com a menor latência. Ideal para aplicativos de banco de dados que suportam logs de banco de dados. Este PSL fornece o maior rendimento porque os logs do banco de dados são extremamente intermitentes e o registro está em constante demanda.	1	45056	22528	4000

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 compartilhados de banco de dados	Fornecer alta taxa de transferência com a menor latência. Ideal para aplicativos de banco de dados, dados armazenados em um repositório de dados comum, mas compartilhados entre bancos de dados.	1	32768	16384	2000
Extremo para dados de banco de dados	Fornecer alto rendimento com a menor latência. Ideal para dados de aplicativos de banco de dados, como informações de tabelas de banco de dados e metadados.	1	24576	12288	2000

Criar e editar níveis de serviço de desempenho

Quando os Níveis de Serviço de Desempenho definidos pelo sistema não correspondem aos requisitos da sua carga de trabalho, você pode criar seus próprios Níveis de Serviço de Desempenho otimizados para suas cargas de trabalho.

Antes de começar

- Você deve ter a função de Administrador do Aplicativo.
- 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 Desempenho personalizados na página Níveis de Serviço de

Desempenho, definindo os objetivos de nível de serviço necessários para os aplicativos que acessarão o armazenamento.



Não é possível modificar um Nível de Serviço de Desempenho se ele estiver atualmente atribuído a uma carga de trabalho.

Passos

- 1. No painel de navegação esquerdo, em **Configurações**, selecione **Políticas > Níveis de serviço de desempenho**.
- 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 Desempenho	Clique em Adicionar .
Editar um Nível de Serviço de Desempenho existente	Selecione um Nível de Serviço de Desempenho existente e clique em Editar .

A página para adicionar ou editar um Nível de Serviço de Desempenho é exibida.

- 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.

Você pode aplicar o novo ou alterado Nível de Serviço de Desempenho às cargas de trabalho (LUNs, Compartilhamentos de Arquivos NFS, Compartilhamentos CIFS) na página Cargas de Trabalho ou ao provisionar uma nova carga de trabalho.

Gerenciar políticas de eficiência de armazenamento

Uma Política de Eficiência de Armazenamento (SEP) permite definir as características de eficiência de armazenamento de uma carga de trabalho. Você pode atribuir um SEP a uma carga de trabalho ao criá-la inicialmente ou depois editando a carga de trabalho.

A eficiência de armazenamento inclui o uso de tecnologias como provisionamento fino, deduplicação e compactação de dados que aumentam a utilização do armazenamento e diminuem os custos de armazenamento. Ao criar SEPs, você pode usar essas tecnologias de economia de espaço individualmente ou em conjunto para atingir a máxima eficiência de armazenamento. Quando você associa as políticas às suas cargas de trabalho de armazenamento, as configurações de política especificadas são atribuídas a elas. O Unified Manager permite que você atribua SEPs definidos pelo sistema e pelo usuário para otimizar os recursos de armazenamento no seu 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 armazenamento 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 um SEP definido pelo sistema ou que esteja atualmente atribuído a uma carga de trabalho. Não é possível excluir um SEP atribuído a uma carga de trabalho ou se ele for o único 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 pelo usuário.
Reserva Espacial	Se o volume é provisionado de forma fina ou espessa.
Desduplicação	Se a desduplicação está habilitada na carga de trabalho: • Em linha: a desduplicação ocorre durante a gravação na carga de trabalho • Contexto: A desduplicação ocorre na carga de trabalho • Desativar: a desduplicação está desativada na carga de trabalho
Compressão	Se a compactação de dados está habilitada na carga de trabalho: • Em linha: a compactação de dados ocorre durante a gravação na carga de trabalho • Contexto: A compressão de dados ocorre na carga de trabalho • Desativar: a compactação de dados é desativada na carga de trabalho
Cargas de trabalho	Número de cargas de trabalho de armazenamento que foram atribuídas ao SEP

Diretrizes para criar uma Política de Eficiência de Armazenamento personalizada

Se os SEPs existentes não atenderem aos requisitos de política para suas cargas de trabalho de armazenamento, você poderá criar um SEP personalizado. No entanto, é recomendável que você tente usar os SEPs definidos pelo sistema para suas cargas de trabalho de armazenamento e crie SEPs personalizados somente se necessário.

Você pode visualizar o SEP atribuído às cargas de trabalho na página Todas as cargas de trabalho e na página Detalhes do volume/integridade. Você pode visualizar a taxa de redução de dados no nível do cluster (sem cópias de instantâneo) com base nessas eficiências de armazenamento no painel Capacidade no Painel e na exibição Capacidade: Todos os clusters.

Criar e editar políticas de eficiência de armazenamento

Quando as Políticas de Eficiência de Armazenamento definidas pelo sistema não correspondem aos seus requisitos de carga de trabalho, você pode criar suas próprias

Políticas de Eficiência de Armazenamento otimizadas para suas cargas de trabalho.

Antes de começar

- Você deve ter a função de Administrador do Aplicativo.
- 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 Armazenamento personalizadas na página Políticas de Eficiência de Armazenamento, definindo as características de eficiência de armazenamento necessárias para os aplicativos que acessarão o armazenamento.



Não é possível modificar uma Política de Eficiência de Armazenamento se ela estiver atualmente atribuída a uma carga de trabalho.

Passos

1. No painel de navegação esquerdo, em **Configurações**, selecione **Políticas > Eficiência de armazenamento**.
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 Armazenamento	Clique em Adicionar
Editar uma Política de Eficiência de Armazenamento existente	Selecione uma Política de Eficiência de Armazenamento existente e clique em Editar

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 Política de Eficiência de Armazenamento nova ou alterada às cargas de trabalho (LUNs, Compartilhamentos de Arquivos NFS, Compartilhamentos CIFS) na página Cargas de Trabalho ou ao provisionar uma nova carga de trabalho.

Gerenciar e monitorar configurações do MetroCluster

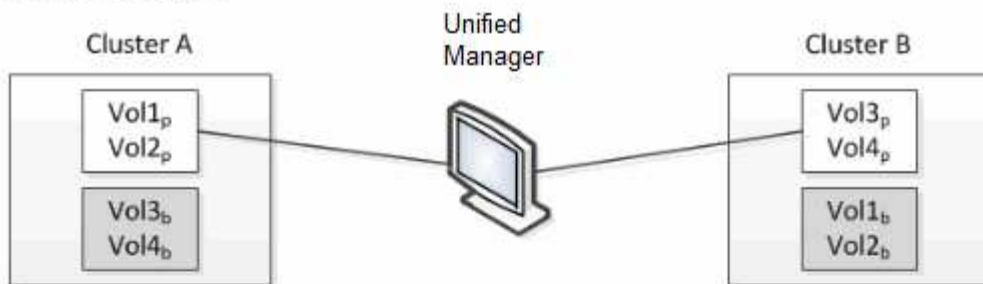
O suporte de monitoramento para configurações do MetroCluster na interface de usuário da Web do Unified Manager permite que você verifique se há problemas de conectividade no seu MetroCluster por meio de configurações de FC e IP. Descobrir um problema de conectividade precocemente permite que você gerencie suas configurações do MetroCluster de forma eficaz.

Comportamento do volume durante a comutação e o retorno

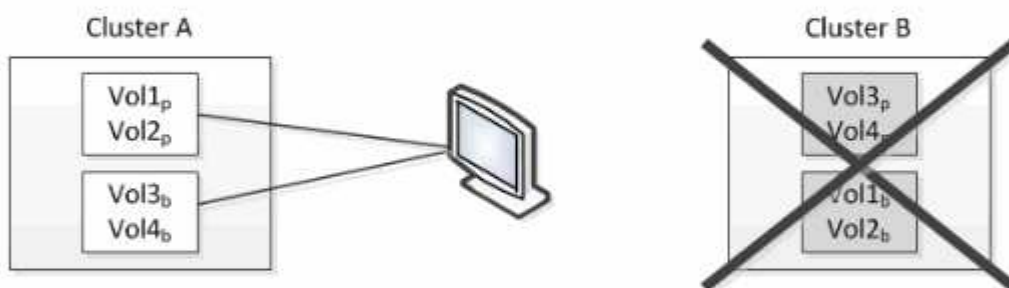
Eventos que acionam uma alternância ou retorno fazem com que volumes ativos sejam movidos de um cluster para outro no grupo de recuperação de desastres. Os volumes no cluster que estavam ativos e fornecendo dados aos clientes são interrompidos, e os volumes no outro cluster são ativados e começam a fornecer dados. O Unified Manager monitora apenas os volumes que estão ativos e em execução.

Como os volumes são movidos de um cluster para outro, é recomendável monitorar ambos os clusters. Uma única instância do Unified Manager pode monitorar ambos os clusters em uma configuração 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:

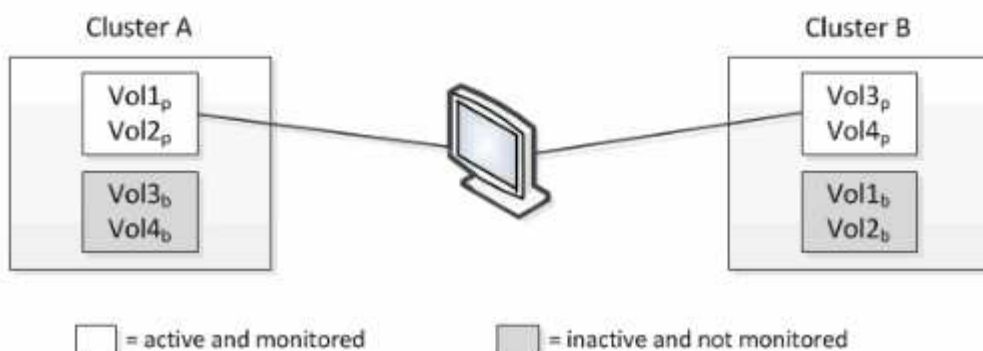
Normal operation



Cluster B fails --- switchover to Cluster A



Cluster B is repaired --- switchback to Cluster B



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 a operação normal:

- O cluster A tem dois volumes ativos: Vol1p e Vol2p.
- O cluster B tem dois volumes ativos: Vol3p e Vol4p.
- O cluster A tem dois volumes inativos: Vol3b e Vol4b.
- O cluster B tem dois volumes inativos: Vol1b e Vol2b.

Informações referentes a cada um dos volumes ativos (estatísticas, eventos e assim por diante) são coletadas pelo Unified Manager. As estatísticas Vol1p e Vol2p são coletadas pelo Cluster A, e as estatísticas Vol3p e Vol4p são coletadas pelo Cluster B.

Após uma falha catastrófica causar uma troca de volumes ativos do Cluster B para o Cluster A:

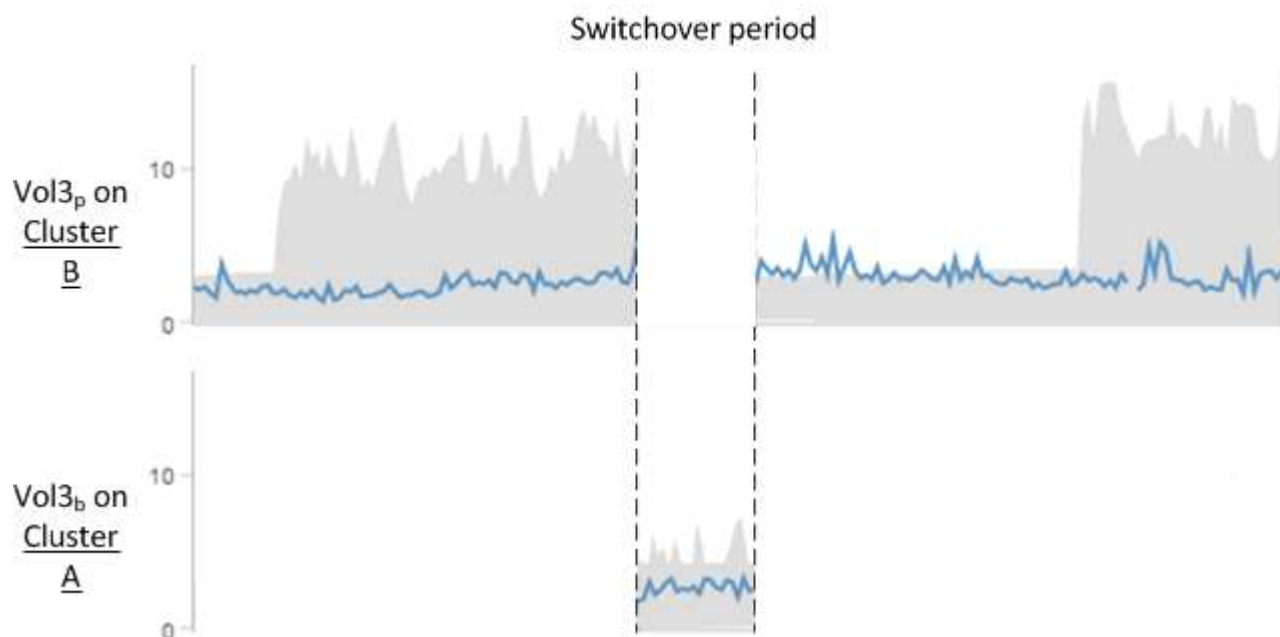
- O cluster A tem quatro volumes ativos: Vol1p, Vol2p, Vol3b e Vol4b.
- O cluster B tem quatro volumes inativos: Vol3p, Vol4p, Vol1b e Vol2b.

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 no Unified Manager para Vol3p não são as mesmas do Vol3b:

- Durante a mudança para o Cluster A, as estatísticas e eventos do Vol3p não ficam visíveis.
- Na primeira troca, o Vol3b parece um novo volume sem informações históricas.

Quando o Cluster B é reparado e uma troca é realizada, o Vol3p fica ativo novamente no Cluster B, com as estatísticas históricas e uma lacuna de estatísticas para o período durante a troca. Vol3b não pode ser visualizado no Cluster A até que outra troca ocorra:





- Os volumes do 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 Unified Manager estiver monitorando ambos os clusters em uma configuração MetroCluster, a pesquisa de volume retornará informações para qualquer volume que esteja ativo naquele momento. Por exemplo, uma busca por "Vol3" retornaria estatísticas e eventos para Vol3b no Cluster A se uma troca tivesse ocorrido e Vol3 tivesse se tornado ativo no Cluster A.

Definições de status de conectividade de cluster para configuração do MetroCluster sobre FC

A conectividade entre os clusters em uma configuração MetroCluster sobre FC pode ter um dos seguintes status: Ótimo, Impactado ou Inativo. Entender os status de conectividade permite que você gerencie suas configurações do MetroCluster de forma eficaz.

Status de conectividade	Descrição	Ícone exibido
Ótimo	A conectividade entre os clusters na configuração do MetroCluster é normal.	
Impactado	Um ou mais erros comprometem o status de disponibilidade de failover; no entanto, ambos os clusters na configuração do MetroCluster ainda estão ativos. Por exemplo, quando o link ISL está inativo, quando o link IP entre clusters está inativo ou quando o cluster parceiro não está acessível.	
Abaixo	A conectividade entre os clusters na configuração do MetroCluster está inativa porque um ou ambos os clusters estão inativos ou estão no modo de failover. Por exemplo, quando o cluster de parceiros está inativo devido a um desastre ou quando há uma troca planejada para fins de teste.	Troca com erros: Mudança bem-sucedida:

Definições de status de espelhamento de dados para MetroCluster sobre FC

As configurações do MetroCluster sobre FC fornecem espelhamento de dados e a capacidade adicional de iniciar um failover se um site inteiro ficar indisponível. O status do espelhamento de dados entre os clusters em uma configuração MetroCluster sobre FC pode ser Normal ou Espelhamento indisponível. Entender o status permite que você gerencie suas configurações do MetroCluster de forma eficaz.

Status de espelhamento de dados	Descrição	Ícone exibido
Normal	O espelhamento de dados entre os clusters na configuração do MetroCluster é normal.	
Espelhamento indisponível	O espelhamento de dados entre os clusters na configuração do MetroCluster não está disponível devido à alternância. Por exemplo, quando o cluster de parceiros está inativo devido a um desastre ou quando há uma troca planejada para fins de teste.	Troca com erros:  Mudança bem-sucedida: 

Monitorar configurações do MetroCluster

Você pode monitorar problemas de conectividade na configuração do MetroCluster . Os detalhes incluem o status dos componentes e a conectividade dentro de um cluster e o status de conectividade entre os clusters na configuração do MetroCluster . Aqui, você aprenderá como monitorar problemas de conectividade em clusters protegidos pelas configurações MetroCluster sobre FC e MetroCluster sobre IP.

Você pode monitorar as configurações do MetroCluster nas seguintes visualizações do painel de navegação esquerdo do Active IQ Unified Manager :

- **Armazenamento > Clusters > Proteção: MetroCluster** view
- **Proteção > Relacionamentos > Relacionamento: MetroCluster** visualizar

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 locais e remotos em uma configuração MetroCluster devem ser adicionados ao Active IQ Unified Manager.

- Em uma configuração do MetroCluster sobre IP, se um Mediador for suportado, o Mediador deverá ser configurado e adicionado ao cluster pela API correspondente.
- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Monitorar problemas de conectividade no MetroCluster por meio da configuração FC

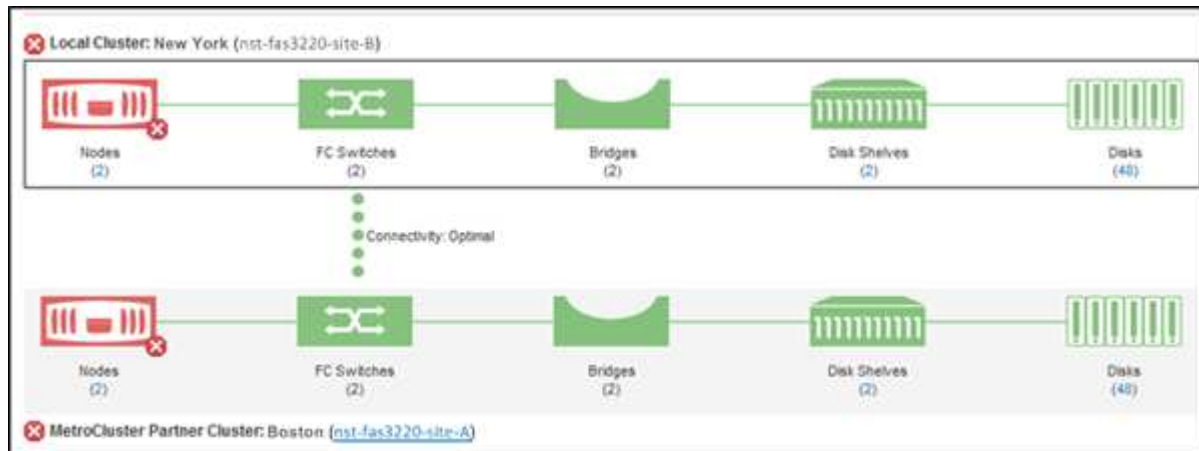
Para clusters em uma configuração MetroCluster sobre FC, os gráficos de conectividade são exibidos na página de detalhes **Cluster / Saúde**. Siga estes passos.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Clusters**.

Uma lista de todos os clusters monitorados é exibida.

2. Na exibição **Proteção: MetroCluster**, clique no nome do cluster para o qual você deseja visualizar os detalhes da configuração do MetroCluster sobre FC. Como alternativa, você pode filtrar por clusters em uma configuração MetroCluster .
3. Na página de detalhes **Cluster / Saúde**, clique na aba * Conectividade do MetroCluster *. A aba * Conectividade MetroCluster * está disponível somente para configurações MetroCluster sobre FC.



A topologia da configuração do MetroCluster é exibida na área de objeto do cluster correspondente. Você pode usar as informações exibidas na página Detalhes do cluster/integridade 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 será exibido:



Se você mover o ponteiro sobre o ícone, poderá visualizar informações detalhadas sobre o evento gerado.

Se você descobrir problemas de conectividade na configuração do MetroCluster , deverá efetuar login no Gerenciador do Sistema ou acessar o ONTAP CLI para resolver os problemas.

Para obter mais informações sobre como determinar a integridade do cluster, consulte ["Determinar a integridade do cluster no MetroCluster por meio da configuração FC"](#) .

Monitorar problemas de conectividade na configuração do 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 **Armazenamento > Clusters**.

Uma lista de todos os clusters monitorados é exibida.

2. Na exibição **Proteção: MetroClusters**, clique no nome do cluster para o qual você deseja visualizar os detalhes da configuração do MetroCluster sobre IP. Como alternativa, você pode filtrar por clusters em uma configuração MetroCluster.
3. Expanda a linha clicando no cursor ▾ ícone. O ícone de circunflexo aparece apenas para um cluster protegido pela configuração MetroCluster sobre IP.

Você pode visualizar a topologia dos sites de origem e espelho, bem como o Mediador, se houver, usado para a conexão. Você pode visualizar as seguintes informações:

- Conectividade entre os sites
- Problemas de saúde e disponibilidade, se houver, em ambos os sites
- Questões relacionadas ao mediador
- Problemas relacionados à replicação.



Os seguintes status são relatados: 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 conectividade entre os clusters de origem e destino não está disponível, e o Mediador entre eles não está configurado.



4. Clique no ícone de status. Uma mensagem com a definição do erro é exibida. Se um evento tiver sido gerado para o problema na sua configuração do MetroCluster sobre IP, você pode clicar no botão **Exibir evento** na mensagem e visualizar os detalhes do evento. Quando você tiver resolvido o problema e o evento, o ícone de status nesta topologia voltará ao normal (✅).
5. Você pode visualizar 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 visualizar a topologia do cluster na página **Clusters**. Para clusters em uma configuração MetroCluster sobre FC, a topologia é exibida na guia * Conectividade do MetroCluster * na página de detalhes * Cluster / Saúde *.

Informações relacionadas

- ["Página de detalhes do cluster/saúde"](#)
- Para obter informações sobre a visualização **Relacionamento: MetroCluster**, consulte ["Monitorar configurações do MetroCluster"](#).
- Para obter informações sobre a visualização **Relacionamento: Status de transferência do último mês**, consulte ["Relacionamento: Visualização do status de transferência do último mês"](#).
- Para obter informações sobre a visualização **Relacionamento: Taxa de transferência do último mês**, consulte ["Relacionamento: Visualização da taxa de transferência do último mês"](#).
- Para obter informações sobre a visualização **Relacionamento: Todos os relacionamentos**, consulte ["Relacionamento: Visualização de todos os relacionamentos"](#).

Monitorar a replicação do MetroCluster

Você pode monitorar e diagnosticar a condição geral de saúde das conexões lógicas enquanto espelha os dados. Você pode identificar os problemas ou qualquer risco que interrompa o espelhamento de componentes do cluster, como agregados, nós e máquinas virtuais de armazenamento.

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

Tanto o cluster local quanto o remoto na configuração do MetroCluster devem ser adicionados ao Unified Manager

Exibir replicação para configurações do MetroCluster sobre IP

Para configurações do MetroCluster sobre IP, o status da replicação de dados é exibido na visualização de visualização da topologia para um cluster protegido pelo MetroCluster sobre IP nas seguintes visualizações do painel de navegação esquerdo do Unified Manager:

- **Armazenamento > Clusters > Proteção: MetroCluster** view
- **Proteção > Relacionamentos > Relacionamento: MetroCluster** visualizar

Para obter informações, consulte ["Monitorar problemas de conectividade no MetroCluster por IP"](#).

Exibir replicação para MetroCluster sobre configurações de FC

Siga estas etapas para determinar quaisquer problemas na replicação de dados para a configuração do MetroCluster sobre FC.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Clusters**.

Uma lista dos clusters monitorados é exibida.

2. Na exibição **Saúde: Todos os clusters**, clique no nome do cluster para o qual você deseja visualizar os detalhes de replicação do MetroCluster . Na página **Detalhes do cluster/saúde**, clique na guia ***Replicação do MetroCluster ***.

A topologia da configuração do MetroCluster a ser replicada é exibida no site local na área de objeto do cluster correspondente com as informações sobre o site remoto onde os dados estão sendo espelhados. Se você mover o ponteiro sobre o ícone, poderá visualizar informações detalhadas sobre o evento gerado.

Você pode usar as informações exibidas na página Detalhes do cluster/integridade para corrigir quaisquer problemas de replicação. Se você descobrir problemas de espelhamento na configuração do MetroCluster , deverá efetuar login no Gerenciador do Sistema ou acessar o ONTAP CLI para resolver os problemas.

Informações relacionadas

["Página de detalhes do cluster/saúde"](#)

Gerenciar 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 pode usar. Você pode visualizar informações de cota de usuários e grupos de usuários, como o uso de disco e arquivo e os vários limites definidos nos discos.

Quais são os limites de cota

Os limites de cota do 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 flexível for ultrapassado ou se o limite rígido for atingido, o servidor do Unified Manager gerará eventos de cota de usuário.

Por padrão, o servidor do Unified Manager envia um e-mail de notificação aos usuários que ultrapassaram o limite flexível da cota ou atingiram o limite rígido da cota e para os quais eventos de cota do usuário estão configurados. Usuários com a função de Administrador do Aplicativo podem configurar alertas que notificam os destinatários especificados sobre eventos de cota do usuário ou grupo de usuários.

Você pode especificar limites de cota usando o ONTAP System Manager ou o ONTAP CLI.

Exibir cotas de usuários e grupos de usuários

A página Detalhes da VM de armazenamento/Integridade exibe informações sobre as cotas de usuários e grupos de usuários configuradas na SVM. Você pode visualizar 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

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > VMs de armazenamento**.
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"](#)

Crie regras para gerar endereços de e-mail

Você pode criar regras para especificar o endereço de e-mail com base na cota de usuários 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

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter revisado as diretrizes na página Regras para gerar endereços de e-mail de cota de usuários e grupos.

Você deve definir as regras para endereços de e-mail de cota e inseri-las na ordem em que deseja executá-las. Por exemplo, se você quiser usar o endereço de e-mail abc@xyz.com para receber notificações sobre violações de cota para abc e usar o endereço de e-mail dl-\$GROUP@\$DOMAIN para todos os outros grupos, as regras devem ser listadas na seguinte ordem:

- se (\$USER == 'abc') então abc@xyz.com
- se (\$GROUP == *) então dl-\$GROUP@\$DOMAIN

Se nenhum dos critérios para as regras especificadas for atendido, a regra padrão será usada:

se (\$USER_OR_GROUP == *) então \$USER_OR_GROUP@\$DOMAIN

Passos

1. No painel de navegação esquerdo, clique em **Geral > Regras de cota de e-mail**.
2. Insira a regra com base em seus critérios.
3. Clique em **Validar** para validar a sintaxe da regra.

Uma mensagem de erro será 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 **VM / Integridade** do armazenamento.

Crie 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 enviados a um usuário ou grupo de usuários quando há um problema relacionado à cota (limite flexível violado ou limite rígido atingido).

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Formato de e-mail de cota**.
2. Insira ou modifique os detalhes nos campos **De**, **Assunto** e **Detalhes do e-mail**.
3. Clique em **Visualizar** 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**.

Editar endereços de e-mail de cotas de usuários e grupos

Você pode modificar os endereços de e-mail com base na cota de usuários 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

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter revisado o ["diretrizes para 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 ao 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 **Armazenamento > SVMs**.
2. Na exibição **Saúde: Todas as VMs de armazenamento**, selecione uma 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	a. Exclua o endereço de e-mail no campo Endereço de e-mail. b. Clique em Salvar. 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 Endereço de e-mail.

Se...	Então...
Você deseja que as notificações sejam enviadas para um endereço de e-mail específico	a. Modifique o endereço de e-mail no campo Endereço de e-mail. b. Clique em Salvar. As regras para gerar endereços de e-mail de cota de usuário e grupo não são mais aplicáveis à cota.

Entenda mais sobre cotas

Entender os conceitos sobre cotas ajuda você a gerenciar suas cotas de usuários e cotas de grupos de usuários com eficiência.

Visão geral do processo de cotas

As cotas podem ser suaves ou rígidas. Cotas flexíveis fazem com que o ONTAP envie uma notificação quando limites especificados são excedidos, e cotas rígidas impedem que uma operação de gravação seja bem-sucedida quando limites especificados são 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 naquele volume para o usuário ou grupo de usuários e determina o seguinte:

- Se o limite rígido será atingido

Em caso afirmativo, a operação de gravação falhará quando o limite máximo for atingido e a notificação de cota máxima for enviada.

- Se o limite suave será violado

Em caso afirmativo, a operação de gravação será bem-sucedida quando o limite flexível for violado e a notificação de cota flexível for enviada.

- Se uma operação de gravação não excederá o limite flexível

Se sim, a operação de gravação será bem-sucedida e nenhuma notificação será 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 FlexVol , para fornecer notificações quando o uso de recursos atingir níveis específicos ou para rastrear o uso de 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
- Para avisar os usuários quando o uso do disco ou do arquivo estiver alto

Descrição das caixas de diálogo de 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 por e-mail que é enviada quando ocorre um problema relacionado à cota e para configurar regras para especificar endereços de e-mail com base na cota do 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 a um usuário ou grupo de usuários quando há um problema relacionado à cota (limite flexível violado ou limite rígido atingido).

A notificação por e-mail é enviada somente quando os seguintes eventos de cota de usuário ou grupo de usuários são gerados: Limite flexível de espaço em disco de cota de usuário ou grupo violado, Limite flexível de contagem de arquivos de cota de usuário ou grupo violado, Limite rígido de espaço em disco de cota de usuário ou grupo atingido ou Limite rígido de contagem de arquivos de cota de usuário ou grupo atingido.

- **De**

Exibe o endereço de e-mail de onde 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 de acordo com suas necessidades. Por exemplo, você pode fornecer informações relacionadas aos atributos de cota e reduzir o número de palavras-chave. Entretanto, você não deve modificar as palavras-chave.

Palavras-chave válidas são as seguintes:

- **\$EVENT_NAME**

Especifica o nome do evento que causou a notificação por e-mail.

- **\$QUOTA_TARGET**

Especifica a qtree ou volume no qual a cota é aplicável.

- **\$QUOTA_USED_PERCENT**

Especifica a porcentagem do limite rígido do disco, limite flexível do disco, limite rígido do arquivo ou limite flexível do arquivo que é usado pelo usuário ou grupo de usuários.

- **\$QUOTA_LIMIT**

Especifica o limite rígido do disco ou limite flexível do disco que é atingido pelo usuário ou grupo de usuários e um dos seguintes eventos é gerado:

- Limite máximo de espaço em disco de cota de usuário ou grupo atingido
- Limite de espaço em disco de cota de usuário ou grupo atingido
- Limite máximo de contagem de arquivos de cota de usuário ou grupo atingido
- Limite flexível de contagem de arquivos de cota de usuário ou grupo atingido

- **\$QUOTA_USED**

Especifica o espaço em disco usado ou o número de arquivos criados pelo usuário ou grupo de usuários.

- **\$QUOTA_USER**

Especifica o nome do usuário ou grupo de usuários.

Botões de comando

Os botões de comando permitem que você visualize, salve ou cancele as alterações feitas no formato de notificação por e-mail:

- **Prévia**

Exibe uma prévia do e-mail de notificação.

- **Restaurar para os padrões de fábrica**

Permite restaurar o formato de notificação para os valores padrão de fábrica.

- **Salvar**

Salva as alterações feitas no formato de notificação.

Página Regras para gerar endereço de e-mail de cota de usuário e grupo

A página Regras para gerar endereços de e-mail de cota de usuários e grupos permite que você crie regras para especificar endereços de e-mail com base na cota de usuários 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 atendido, o critério para a próxima regra será 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. Entretanto, você não pode alterar a ordem da regra padrão.

Por exemplo, se você quiser usar o endereço de e-mail qtree1@xyz.com para receber notificações sobre violações de cota para qtree1 e usar o endereço de e-mail admin@xyz.com para todos os outros qtrees, as regras devem ser listadas na seguinte ordem:

- se (\$QTREE == 'qtree1') então qtree1@xyz.com
- se (\$QTREE == *) então admin@xyz.com

Se nenhum dos critérios para as regras especificadas for atendido, a regra padrão será usada:

se (\$USER_OR_GROUP == *) então \$USER_OR_GROUP@\$DOMAIN

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 das regras

A sintaxe da regra deve ser uma das seguintes:

- se (valid variableoperator *) então email ID@domain name

if é uma palavra-chave e está em letras 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 \$DOMAIN ou uma combinação de qualquer caractere e a variável válida \$DOMAIN. Variáveis válidas podem estar em maiúsculas ou minúsculas, mas não devem ser uma combinação de ambas. Por exemplo, \$domain e \$DOMAIN são válidos, mas \$Domain não é uma variável válida.

- se (valid variableoperator `string`) então email ID@domain name

if é uma palavra-chave e está em minúsculas. O operador pode ser contains ou ==. 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 \$DOMAIN ou uma combinação de qualquer caractere e a variável válida \$DOMAIN. Variáveis válidas podem estar em maiúsculas ou minúsculas, mas não devem ser uma combinação de ambas. Por exemplo, \$domain e \$DOMAIN são válidos, mas \$Domain não é uma variável válida.

Botões de comando

Os botões de comando permitem que você salve, valide ou cancele as regras criadas:

- **Validar**

Valida a sintaxe da regra criada. Se houver erros durante a validação, a regra que gera o erro será exibida junto com uma mensagem de erro.

- **Restaurar para os padrões de fábrica**

Permite restaurar as regras de endereço para os valores padrão de fábrica.

- **Salvar**

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 será exibida junto com uma mensagem de erro.

Solução de problemas

As informações de solução de problemas ajudam você a identificar e resolver problemas encontrados ao usar o Unified Manager.

Adicionar espaço em disco ao diretório do banco de dados do Unified Manager

O diretório de 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 dos clusters depois que o diretório atinge 95% da capacidade.

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.

Adicionar espaço ao disco de dados da máquina virtual VMware

Se precisar aumentar a quantidade de espaço no disco de dados para o banco de dados do Unified Manager, você 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.
- Você deve ter as credenciais de usuário de manutenção.

Recomendamos que você faça backup da 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 do 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 ocorreu na sua implantação, aumente o espaço do disco que for maior. O disco de dados sempre terá mais espaço que o outro disco.

2. No cliente vSphere, selecione a máquina virtual Unified Manager e, em seguida, selecione a guia **Console**.
3. Clique na janela do console e 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 Tamanho do Disco de Dados**.

Adicionar espaço ao diretório de dados do host Linux

Se você alocou espaço em disco insuficiente para o `/opt/netapp/data` diretório para oferecer suporte ao Unified Manager quando você configurou originalmente o host Linux e depois instalou o Unified Manager, você pode adicionar espaço em disco após a instalação aumentando o espaço em disco no `/opt/netapp/data` diretório.

Antes de começar

Você deve ter acesso de usuário root 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. Efetue 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 atual `/opt/netapp/data` diretório.
4. Copie o conteúdo e a configuração de privilégios do existente `/opt/netapp/data` diretório para o diretório de dados de backup:

```
cp -arp /opt/netapp/data/* /backup-data
```

5. Se o SE Linux estiver habilitado:

- a. Obtenha o tipo SE Linux para pastas existentes `/opt/netapp/data` pasta:

```
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. Expandir o tamanho do `/opt/netapp/data` diretório para um mínimo de 150 GB por meio de comandos LVM ou adicionando discos extras.



Se você criou `/opt/netapp/data` 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, como `resize` e `extend` pode não funcionar como esperado.

8. Confirme que o `/opt/netapp/data` o proprietário do diretório (`mysql`) e o grupo (`root`) não foram alterados:

```
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 habilitado, confirme se o contexto para o `/opt/netapp/data` o 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. Excluir o arquivo `abc` para que esse arquivo estranho não cause um erro no banco de dados no futuro.

11. Copie o conteúdo de `backup-data` de volta ao expandido `/opt/netapp/data` diretório:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Se o SE Linux estiver habilitado, execute o seguinte comando:

```
chcon -R --type=mysqlld_db_t /opt/netapp/data
```

13. Inicie o serviço MySQL:

```
systemctl start mysqld
```

14. Após o serviço MySQL ser iniciado, inicie os serviços ocie e ocieau na ordem mostrada:

```
systemctl start ocie ocieau
```

15. Depois que todos os serviços forem iniciados, exclua a pasta de backup /backup-data :

```
rm -rf /backup-data
```

Adicionar espaço à unidade lógica do servidor Microsoft Windows

Se precisar aumentar a quantidade de espaço em disco para o banco de dados do Unified Manager, você poderá adicionar capacidade à unidade lógica na qual o Unified Manager está instalado.

Antes de começar

Você deve ter privilégios de administrador do Windows.

Recomendamos que você faça backup do banco de dados do Unified Manager antes de adicionar espaço em disco.

Passos

1. Efetue login como administrador no servidor Windows no qual você deseja adicionar espaço em disco.
2. Siga o passo 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 Unified Manager está instalado.	Siga os passos do tópico da Microsoft: "Estender um volume básico"
Em um servidor físico, adicione uma unidade de disco rígido.	Siga os passos do tópico da Microsoft: "Adicionando unidades de disco rígido"
Em uma máquina virtual, aumente o tamanho de uma partição de disco.	Siga os passos do tópico VMware: "Aumentando o tamanho de uma partição de disco"

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 perceber que as coletas de clusters grandes não estão terminando dentro do tempo padrão. Esta configuração afeta a coleta

de estatísticas de todos os clusters que esta instância do Unified Manager está monitorando.

Antes de começar

Você deve ter um ID de usuário e uma senha autorizados para efetuar login no console de manutenção do servidor do Unified Manager.

O problema das coletas de estatísticas de desempenho não serem concluídas no prazo é indicado 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 configuração por nenhum outro motivo.



Alterar esse valor da configuração padrão de 5 minutos pode afetar o número e a frequência de eventos de desempenho relatados pelo Unified Manager. Por exemplo, limites de desempenho definidos pelo sistema acionam eventos quando a política é excedida por 30 minutos. Ao utilizar coletas de 5 minutos, a política deve ser excedida por seis coletas consecutivas. Para coletas 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 atual de coleta de dados estatísticos.

Passos

1. Efetue login usando SSH como 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 rotulada **Configuração do intervalo de pesquisa de desempenho** e pressione Enter.
3. Se solicitado, digite a senha do usuário de manutenção novamente.
4. Digite o número do novo intervalo de pesquisa que você deseja definir e pressione Enter.

Se você alterou o intervalo de coleta do Unified Manager para 10 ou 15 minutos e tem uma conexão atual com um provedor de dados externo (como o Graphite), você deve alterar o intervalo de transmissão do provedor de dados para que seja igual ou maior que o intervalo de coleta do Unified Manager.

Alterar o período de tempo em que o Unified Manager retém dados de eventos e desempenho

Por padrão, o Unified Manager armazena dados de eventos e dados de desempenho por 6 meses para todos os clusters monitorados. Após esse período, os dados mais antigos são excluídos automaticamente para dar espaço aos novos dados. Esse período 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 opere de maneira ideal.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Você pode alterar os períodos de retenção para esses dois tipos de dados na página Retenção de Dados.

Essas configurações afetam a retenção de dados de todos os clusters que esta instância do Unified Manager está monitorando.



O Unified Manager coleta estatísticas de desempenho a cada 5 minutos. A cada dia, as estatísticas de 5 minutos são resumidas em estatísticas de desempenho por hora. Ele retém 30 dias de dados históricos de desempenho de 5 minutos e 6 meses de dados resumidos de desempenho por hora (por padrão).

Você deve reduzir o período de retenção somente se estiver ficando sem espaço ou se o backup e outras operações estiverem demorando muito para serem concluídos. A redução do período de retenção tem os seguintes efeitos:

- Dados de desempenho antigos são excluídos do banco de dados do Unified Manager após meia-noite.
- Dados de eventos antigos são excluídos do banco de dados do Unified Manager imediatamente.
- Eventos anteriores ao período de retenção não estarão mais disponíveis para visualização na interface do usuário.
- Os locais na interface do usuário onde as estatísticas de desempenho por hora são exibidas ficarão em branco antes do período de retenção.
- Se o período de retenção do evento exceder o período de retenção dos dados de desempenho, uma mensagem será exibida abaixo do controle deslizante de desempenho avisando que eventos de desempenho mais antigos podem não ter dados de suporte 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 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 retidos e clique em **Salvar**.

Erro de autenticação desconhecido

Ao executar 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 Active Directory
- Vincular nome distinto do serviço de autenticação OpenLDAP

Ação corretiva

1. No painel de navegação esquerdo, clique em **Geral > Autenticação Remota**.
2. Com base no serviço de autenticação selecionado, insira as informações apropriadas para Nome do administrador ou Nome distinto do vínculo.
3. Clique em **Testar autenticação** para testar a autenticação com os detalhes que você especificou.
4. Clique em **Salvar**.

Usuário não encontrado

Ao executar 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

Esse problema pode ocorrer se o usuário existir no servidor AD ou no servidor LDAP e se você tiver definido o nome distinto base com um valor incorreto.

Ação corretiva

1. No painel de navegação esquerdo, clique em **Geral > Autenticação Remota**.
2. Insira as informações apropriadas para o nome distinto base.
3. Clique em **Salvar**.

Problema ao adicionar LDAP usando outros serviços de autenticação

Quando você seleciona Outros como o serviço de autenticação, a Classe de objeto do usuário e do grupo mantém os valores do modelo selecionado anteriormente. Se o servidor LDAP não usar os mesmos valores, a operação poderá falhar.

Causa

Os usuários não estão configurados corretamente no OpenLDAP.

Ação corretiva

Você pode corrigir esse problema manualmente usando uma das seguintes soluções alternativas.

Se a classe de objeto de usuário e a classe de objeto de grupo do LDAP forem usuário e grupo, respectivamente, execute as seguintes etapas:

1. No painel de navegação esquerdo, clique em **Geral > Autenticação Remota**.
2. No menu suspenso **Serviço de autenticação**, selecione **Active Directory** e, em seguida, selecione **Outros**.
3. Preencha os campos de texto.

Se a classe de objeto de usuário e a classe de objeto de grupo do LDAP forem `posixAccount` e `posixGroup`, respectivamente, execute as seguintes etapas:

1. No painel de navegação esquerdo, clique em **Geral > Autenticação Remota**.
2. No menu suspenso **Serviço de autenticação**, selecione **OpenLDAP** e, em seguida, selecione **Outros**.
3. Preencha os campos de texto.

Se as duas primeiras soluções alternativas não se aplicarem, ligue para o `option-set API` e defina o `auth.ldap.userObjectClass` e `auth.ldap.groupObjectClass` opções para os valores corretos.

Problema de rotação de log do NetApp Manageability SDK em sistemas Windows

Depois de adicionar um cluster baseado em API ONTAPI ao Unified Manager em um sistema operacional Windows, o `nmsdk.log` o tamanho do arquivo aumenta e excede o limite de 10 MB.

Causa

Esse problema pode ocorrer se a rotação do log não ocorrer.

Ação corretiva

1. Pare o Unified Manager.
2. Ao instalar o Unified Manager no Windows, instale o Logrotate versão 0.0.0.18. Para mais informações, consulte o "[Guia de reforço de segurança para o relatório técnico do NetApp Manageability SDK](#)".
3. Inicie o Unified Manager.

Gerenciar eventos e alertas

Gerenciar eventos

Os eventos ajudam você a identificar problemas nos clusters monitorados.

O que 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 em mensagens do AutoSupport geradas de todos os sistemas de armazenamento monitorados pelo Unified Manager.

Para mais informações, consulte ["Como os eventos da plataforma Active IQ são gerados"](#).

O Unified Manager verifica automaticamente se há um novo arquivo de regras e só baixa um novo arquivo quando há regras mais recentes. Em sites sem acesso à rede externa, você precisa carregar as regras manualmente em **Gerenciamento de armazenamento > Configuração de evento > Carregar regras**.

Esses eventos do Active IQ não se sobrepõem aos eventos existentes do Unified Manager e identificam incidentes ou riscos relacionados à configuração do sistema, cabeamento, práticas recomendadas e problemas de disponibilidade.

Para obter mais informações sobre como habilitar eventos de plataforma, consulte ["Habilitando eventos do portal Active IQ"](#) . Para obter mais informações sobre o upload do arquivo de regras, consulte ["Carregando um novo arquivo de regras do Active IQ"](#) .

O NetApp Active IQ é um serviço baseado em nuvem que fornece análise preditiva e suporte proativo para otimizar as operações do sistema de armazenamento na nuvem híbrida da NetApp . Ver ["NetApp Active IQ"](#) para mais informações.

O que são eventos do Sistema de Gerenciamento de Eventos

O Sistema de Gerenciamento de Eventos (EMS) coleta dados de eventos de diferentes partes do kernel ONTAP e fornece mecanismos de encaminhamento de eventos. Esses eventos ONTAP podem ser relatados como eventos EMS no Unified Manager. O monitoramento e o gerenciamento centralizados facilitam a configuração de eventos críticos de EMS e notificações de alerta com base nesses eventos de 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 relatado assim que o evento ocorre no cluster.

Há 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 individuais do EMS.

Os eventos EMS gerados pelo Unified Manager são relatados de forma diferente dependendo do método em que o evento foi gerado:

Funcionalidade	Mensagens EMS automáticas	Mensagens EMS assinadas
Eventos EMS disponíveis	Subconjunto de eventos EMS	Todos os eventos de EMS
Nome da mensagem EMS quando acionada	Nome do evento do Unified Manager (convertido do nome do evento do EMS)	Não específico no formato "Erro EMS recebido". A mensagem detalhada fornece o formato de notação de ponto do evento EMS real
Mensagens recebidas	Assim que o aglomerado for descoberto	Após adicionar cada evento EMS necessário ao Unified Manager e após o próximo ciclo de pesquisa de 15 minutos
Ciclo de vida do evento	Igual a outros eventos do Unified Manager: estados Novo, Reconhecido, Resolvido e Obsoleto	O evento EMS se torna obsoleto após a atualização do cluster, após 15 minutos, a partir da criação do evento.
Captura eventos durante o tempo de inatividade do Unified Manager	Sim, quando o sistema é inicializado, ele se comunica com cada cluster para adquirir eventos ausentes	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 automáticos do EMS são eventos informativos que indicam que um evento anterior foi resolvido. Por exemplo, o evento informativo "FlexGroup Constituents Space Status All OK" indica que o evento de erro "FlexGroup Constituents Have Space Issues" foi resolvido. 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 se torna obsoleto automaticamente se o mesmo volume receber outro evento de erro "Problemas de espaço".

Eventos EMS 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 seguintes eventos EMS estão disponíveis ao monitorar clusters executando o software ONTAP 9.5 ou superior:

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do Unified Manager
Acesso à camada de nuvem negado para realocação agregada	arl.netra.ca.check.falhou	Agregar	Erro
Acesso à camada de nuvem negado para realocação agregada durante failover de armazenamento	gb.netra.ca.check.falhou	Agregar	Erro
Ressincronização de replicação de espelho do FabricPool concluída	waf1.ca.resync.completo	Conjunto	Erro
Espaço do FabricPool quase cheio	fabricpool.quase.cheio	Conjunto	Erro
Período de carência NVMe-oF iniciado	nvmf.períododegraça.início	Conjunto	Aviso
Período de carência NVMe-oF ativo	nvmf.graceperiod.ativo	Conjunto	Aviso
Período de carência do NVMe-oF expirado	nvmf.graceperiod.expired	Conjunto	Aviso
LUN destruído	lun.destruir	LUN	Informação
Nuvem AWS MetadataConnFail	nuvem.aws.metadataConnFail	Nó	Erro
Nuvem AWS IAMCreds Expirado	cloud.aws.iamCredsExpirados	Nó	Erro
Nuvem AWS IAMCredsInválido	cloud.aws.iamCredsInválido	Nó	Erro
Nuvem AWS IAMCredsNotFound	cloud.aws.iamCredsNãoEncontrados	Nó	Erro
Nuvem AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	Nó	Informação
Nuvem AWS IAMRoleInválido	cloud.aws.iamRoleInválido	Nó	Erro

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do Unified Manager
Nuvem AWS IAMRoleNotFound	nuvem.aws.iamRoleNotFound	Nó	Erro
Host da camada de nuvem não resolvido	objstore.host.inresolvel	Nó	Erro
Interface de rede intercluster da camada de nuvem inativa	objstore.interclusterlifPara baixo	Nó	Erro
Assinatura de nível de nuvem de incompatibilidade de solicitação	osc.signatureMismatch	Nó	Erro
Um dos pools NFSv4 está esgotado	Nblade.nfsV4PoolExhaust	Nó	Crítico
Memória do monitor QoS máxima	qos.monitor.memória.máxima	Nó	Erro
Monitor de QoS com memória reduzida	qos.monitor.memória.abated	Nó	Informação
NVMeNS Destruir	NVMeNS.destruir	Espaço de nomes	Informação
NVMeNS Online	NVMeNS.offline	Espaço de nomes	Informação
NVMeNS Offline	NVMeNS.online	Espaço de nomes	Informação
NVMeNS Fora do Espaço	NVMeNS.fora.do.espaço	Espaço de nomes	Aviso
Replicação síncrona fora de sincronia	sms.status.fora.de.sincronia	Relacionamento SnapMirror	Aviso
Replicação Síncrona Restaurada	sms.status.em.sincronização	Relacionamento SnapMirror	Informação
Falha na ressincronização automática da replicação síncrona	sms.resync.tentativa.falha	Relacionamento SnapMirror	Erro
Muitas conexões CIFS	Nblade.cifsMuitasAutenticações	SVM	Erro

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do Unified Manager
Conexão CIFS máxima excedida	Nblade.cifsMaxOpenSam eFile	SVM	Erro
Número máximo de conexões CIFS por usuário excedido	Nblade.cifsMaxSessPerU srConn	SVM	Erro
Conflito de nome NetBIOS CIFS	Nblade.cifsNbNameConfli to	SVM	Erro
Tentativas de conectar CIFS inexistentes	Nblade.cifsNoPrivShare	SVM	Crítico
Falha na operação de cópia de sombra do CIFS	cifs.shadowcopy.falha	SVM	Erro
Vírus encontrado pelo servidor AV	Nblade.vscanVirus detectado	SVM	Erro
Nenhuma conexão de servidor AV para verificação de vírus	Nblade.vscanNoScanner Conn	SVM	Crítico
Nenhum servidor AV registrado	Nblade.vscanNoRegdSca nner	SVM	Erro
Nenhuma conexão de servidor AV responsiva	Nblade.vscanConnInativo	SVM	Informação
Servidor AV muito ocupado para aceitar nova solicitação de verificação	Nblade.vscanConnPressã o de retorno	SVM	Erro
Tentativa de usuário não autorizado no servidor AV	Nblade.vscanBadUserPriv Access	SVM	Erro
Os constituintes do FlexGroup têm problemas de espaço	flexgroup.constituientes.tê m.problemas.de.espaço	Volume	Erro
Status do espaço dos constituintes do FlexGroup : Tudo OK	flexgroup.constituientes.es paço.status.tudo.ok	Volume	Informação

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do Unified Manager
Os constituintes do FlexGroup têm problemas com inodes	flexgroup.constituents.hav e.inodes.issues	Volume	Erro
Status dos inodes dos constituintes do FlexGroup : Tudo OK	flexgroup.constituientes.inodes.status.all.ok	Volume	Informação
Volume Espaço Lógico Quase Cheio	monitor.vol.nearFull.inc.sav	Volume	Aviso
Volume Espaço Lógico Completo	monitor.vol.full.inc.sav	Volume	Erro
Volume Lógico Espaço Normal	monitor.vol.one.ok.inc.sav	Volume	Informação
Falha no dimensionamento automático do volume WAFL	wafl.vol.autoSize.falha	Volume	Erro
WAFL Volume AutoSize concluído	wafl.vol.autoSize.feito	Volume	Informação
Tempo limite da operação do arquivo WAFL READDIR	wafl.readdir.expired	Volume	Erro

Inscriva-se nos eventos do ONTAP EMS

Você pode assinar para receber eventos do Sistema de Gerenciamento de Eventos (EMS) gerados por sistemas instalados com o software ONTAP . Um subconjunto de eventos de EMS é relatado ao Unified Manager automaticamente, mas eventos de EMS adicionais são relatados somente se você tiver se inscrito nesses eventos.

Antes de começar

Não assine eventos do EMS que já foram adicionados automaticamente ao Unified Manager, pois isso pode causar confusão ao receber dois eventos para o mesmo problema.

Você pode se inscrever em qualquer número de eventos do EMS. Todos os eventos nos 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 ONTAP 9 EMS* fornece informações detalhadas sobre todas as mensagens EMS para a versão especificada do software ONTAP 9. Localize a versão apropriada do *Catálogo de Eventos EMS* na página Documentação do Produto ONTAP 9 para obter uma lista dos eventos aplicáveis.

Você pode configurar alertas para os eventos do ONTAP EMS nos quais você se inscreveu e pode criar scripts personalizados para serem executados para esses eventos.



Se você não receber os eventos do ONTAP EMS nos quais se inscreveu, pode haver um problema com a configuração de DNS do cluster, que está impedindo que o cluster alcance o servidor do Unified Manager. Para resolver esse problema, o administrador do cluster deve corrigir a configuração de DNS do cluster e reiniciar o Unified Manager. Isso liberará os eventos EMS pendentes no servidor do Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de evento**.
2. Na página Configuração de evento, clique no botão **Inscrever-se em eventos do EMS**.
3. Na caixa de diálogo Inscrever-se em eventos do EMS, insira o nome do evento do ONTAP EMS no qual você deseja se inscrever.

Para visualizar os nomes dos eventos EMS aos quais você pode se inscrever, no 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 do ONTAP EMS Event Subscription no Active IQ Unified Manager"

4. Clique em **Adicionar**.

O evento EMS é adicionado à lista de eventos EMS inscritos, 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 em eventos do 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 deverá remover o evento incorreto e adicioná-lo novamente.

Quando o evento ONTAP EMS ocorre, o evento é exibido na página Eventos. Você pode selecionar o evento para ver detalhes sobre o evento do EMS na página 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

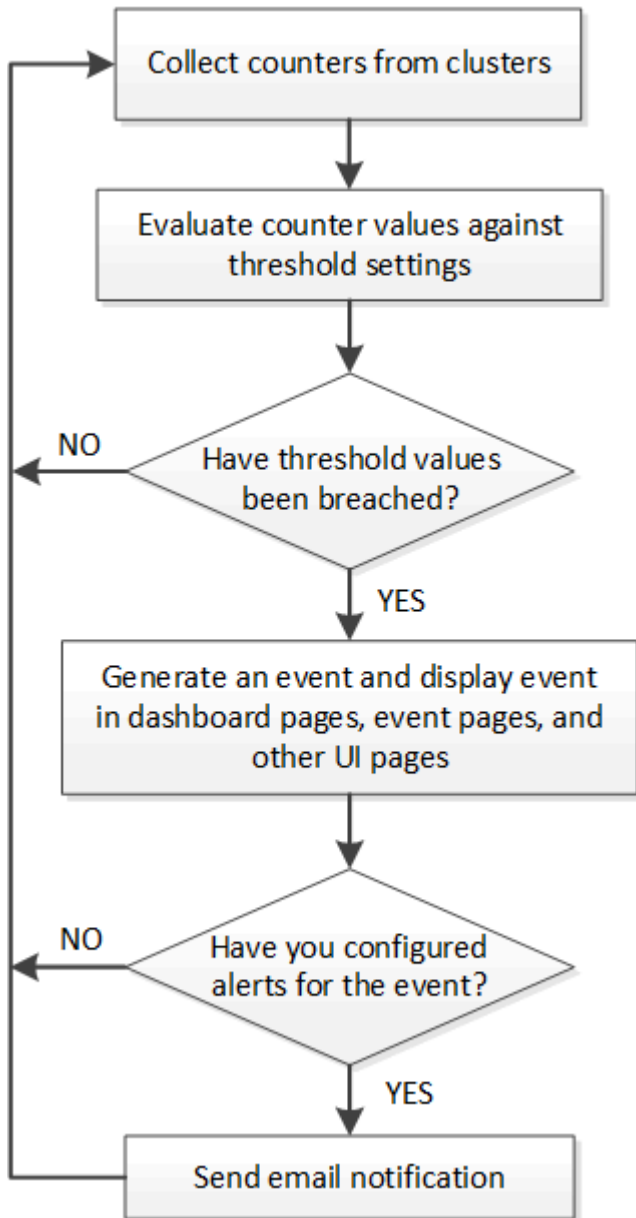
Quando o Unified Manager recebe um evento, ele é exibido na página Painel, na página de inventário do Gerenciamento de Eventos, nas guias Resumo e Explorer da página Cluster/Desempenho e na página de inventário específica do objeto (por exemplo, a página de inventário Volumes/Saúde).

Quando o Unified Manager detecta várias ocorrências contínuas da mesma condição de evento para o mesmo componente de 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 administradores do Unified Manager.
- O evento pode ser enviado para destinatários de e-mail adicionais.
- Uma armadilha SNMP pode ser enviada ao receptor da armadilha.
- Um script personalizado pode ser executado para realizar uma ação.

Esse fluxo de trabalho é mostrado no diagrama a seguir.



Ver eventos e detalhes dos eventos

Você pode visualizar detalhes sobre um evento acionado pelo Unified Manager para tomar medidas corretivas. Por exemplo, se houver um evento de saúde Volume Offline, você pode clicar nesse evento para visualizar os detalhes e executar ações corretivas.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos 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 Reconhecidos (ativos) que foram gerados nos últimos 7 dias e que têm um Nível de Impacto de Incidente ou Risco.

2. Se você quiser visualizar uma categoria específica 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 cujos detalhes você deseja visualizar.

Os detalhes do evento são exibidos na página Detalhes do evento.

Ver eventos não atribuídos

Você pode visualizar eventos não atribuídos e atribuir cada um deles a um usuário que pode resolvê-los.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos 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 o gerou para não continuar recebendo notificações de alerta repetidas. Depois de tomar uma ação corretiva para um evento específico, você deve marcá-lo como resolvido.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode reconhecer e resolver vários eventos simultaneamente.



Você não pode reconhecer eventos de informação.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.
2. Na lista de eventos, execute as seguintes ações para reconhecer os eventos:

Se você quiser...	Faça isso...
Reconhecer e marcar um único evento como resolvido	a. Clique no nome do evento. b. Na página Detalhes do evento, determine a causa do evento. c. Clique em Reconhecer . d. Tome as medidas corretivas apropriadas. e. Clique em Marcar como resolvido .
Reconhecer e marcar vários eventos como resolvidos	a. Determine a causa dos eventos na respectiva página de detalhes do evento. b. Selecione os eventos. c. Clique em Reconhecer . d. Tome as medidas corretivas apropriadas. e. Clique em Marcar como resolvido .

Depois que o evento é marcado como resolvido, ele 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 **Publicar**.

Atribuir eventos a usuários específicos

Você pode atribuir eventos não atribuídos a si 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 armazenamento, você pode atribuir os eventos desses problemas ao usuário que gerencia esse objeto.

Antes de começar

- O nome do usuário e o ID de e-mail devem ser configurados corretamente.
- Você deve ter a função de Operador, Administrador de Aplicativos 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 você quiser atribuir o evento a...	Então faça isto...
Você mesmo	Clique em Atribuir a > Eu .

Se você quiser atribuir o evento a...	Então faça isto...
Outro usuário	a. Clique em Atribuir a > Outro usuário. b. Na caixa de diálogo Atribuir proprietário, insira o nome do usuário ou selecione um usuário na lista suspensa. c. Clique em Atribuir. Uma notificação por e-mail é enviada ao usuário.  Se você não inserir um nome de usuário ou selecionar um usuário na lista suspensa e clicar em Atribuir, o evento permanecerá não atribuído.

Desativar eventos indesejados

Todos os eventos são ativados por padrão. Você pode desabilitar eventos globalmente para evitar a geração de notificações para eventos que não são importantes no seu ambiente. Você pode habilitar eventos que estão desabilitados quando quiser voltar a receber notificações sobre eles.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Quando você desabilita eventos, os eventos gerados anteriormente no sistema são marcados como obsoletos, e os alertas configurados para esses eventos não são acionados. Quando você habilita eventos que estão desabilitados, as notificações para esses eventos são geradas a partir do próximo ciclo de monitoramento.

Quando você desabilita um evento para um objeto (por exemplo, o `vol offline` evento) e, depois, você habilita o evento, o Unified Manager não gera novos eventos para objetos que ficaram offline quando o evento estava no estado desabilitado. O Unified Manager gera um novo evento somente quando há uma alteração no estado do objeto após o evento ter sido reativado.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de evento**.
2. Na página **Configuração de eventos**, desabilite ou habilite eventos escolhendo uma das seguintes opções:

Se você quiser...	Então faça isto...
Desativar eventos	a. Clique em Desativar. b. Na caixa de diálogo Desativar eventos, selecione a gravidade do evento. c. Na coluna Eventos correspondentes, selecione os eventos que você deseja desabilitar com base na gravidade do evento e clique na seta para a direita para mover esses eventos para a coluna Desabilitar eventos. d. Clique em Salvar e Fechar. e. Verifique se os eventos que você desativou são exibidos na exibição de lista da página Configuração de eventos.
Habilitar eventos	a. Marque a caixa de seleção do evento ou eventos que você deseja habilitar. b. Clique em Ativar.

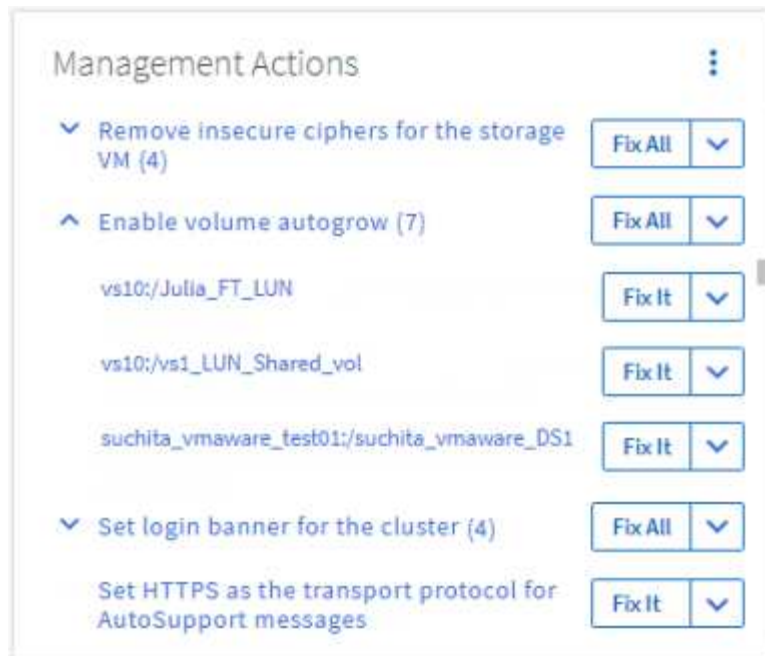
Corrigir problemas usando a correção automática do Unified Manager

Há certos eventos que o Unified Manager pode diagnosticar completamente e fornecer uma única resolução usando o botão **Corrigir**. Quando disponíveis, essas resoluções são exibidas no Painel, 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 Detalhes do evento para que você possa implementar a melhor solução usando o ONTAP System Manager ou o ONTAP CLI. Uma ação **Corrigir** está disponível quando o Unified Manager determina que há uma única resolução para corrigir o problema e que ele pode ser resolvido usando um comando ONTAP CLI.

Passos

1. Para visualizar eventos que podem ser corrigidos no **Painel**, clique em **Painel**.



2. Para resolver qualquer um dos problemas que o Unified Manager pode corrigir, clique no botão **Corrigir**. 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, consulte "[Quais problemas o Unified Manager pode corrigir](#)".

Habilitar e desabilitar relatórios de eventos do Active IQ

Os eventos da plataforma Active IQ são gerados e exibidos na interface do usuário do Unified Manager por padrão. Se você achar que esses eventos são muito "barulhentos" ou que não deseja visualizá-los no Unified Manager, você pode desabilitar a geração desses eventos. Você pode habilitá-los mais tarde se quiser voltar a receber essas notificações.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Quando você desabilita esse recurso, o Unified Manager para de receber eventos da plataforma Active IQ imediatamente.

Quando você habilita 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. O horário de início é baseado em quando o Unified Manager recebe mensagens do AutoSupport de cada cluster.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Configurações de recursos**.
2. Na página **Configurações de recursos**, desabilite ou habilite os eventos da plataforma Active IQ escolhendo uma das seguintes opções:

Se você quiser...	Então faça isto...
Desativar eventos da plataforma Active IQ	No painel * Eventos do Portal Active IQ *, mova o botão deslizante para a esquerda.
Habilitar eventos da plataforma Active IQ	No painel * Eventos do Portal Active IQ *, mova o botão deslizante para a direita.

Carregar um novo arquivo de regras do Active IQ

O Unified Manager verifica automaticamente se há um novo arquivo de eventos (regras) do Active IQ e baixa um novo arquivo quando há regras mais recentes. No entanto, em sites sem acesso à rede externa, você precisa carregar o arquivo de regras manualmente.



As regras do Active IQ também são chamadas de regras seguras do Config Advisor (CA).

Ao instalar ou atualizar o Unified Manager para uma versão específica em um site sem conectividade de rede, as regras do Active IQ incluídas ficam automaticamente disponíveis para upload. No entanto, é recomendável que você baixe um novo arquivo de regras aproximadamente uma vez por mês no site de suporte da NetApp para garantir que eventos atualizados sejam gerados e que seus sistemas de armazenamento continuem funcionando perfeitamente.

Antes de começar

- O relatório de eventos do portal Active IQ deve estar habilitado. Este recurso é habilitado por padrão. Para obter informações, consulte "[Habilitando eventos do portal Active IQ](#)".
- 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

Passos

1. Em um computador com acesso à rede, navegue até o site de suporte da NetApp e baixe as regras atuais .zip arquivo.

O pacote de regras inclui o repositório de regras, fontes de dados e um artigo da base de conhecimento da NetApp.



Em sistemas Windows, em um site sem conectividade de rede, o artigo da KB da NetApp não é incluído 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 com todas as regras.

2. Transfira o arquivo de regras para alguma mídia que você possa levar para a área segura e depois copie-o para um sistema na área segura.
3. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de evento**.
4. Na página **Configuração do evento**, clique no botão **Carregar regras**.

5. Na caixa de diálogo **Regras de upload**, navegue e selecione as regras .zip arquivo que você baixou e clique em **Upload**.

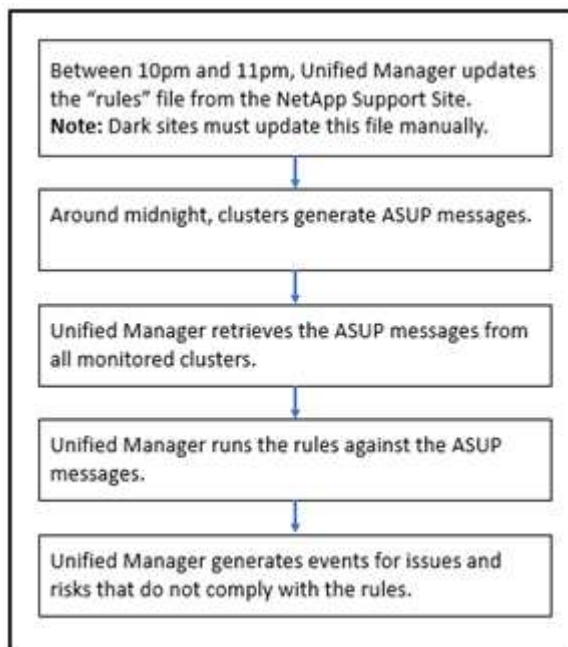
Este processo pode levar alguns minutos.

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 Conhecimento (KB): ["Como atualizar as regras do 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.

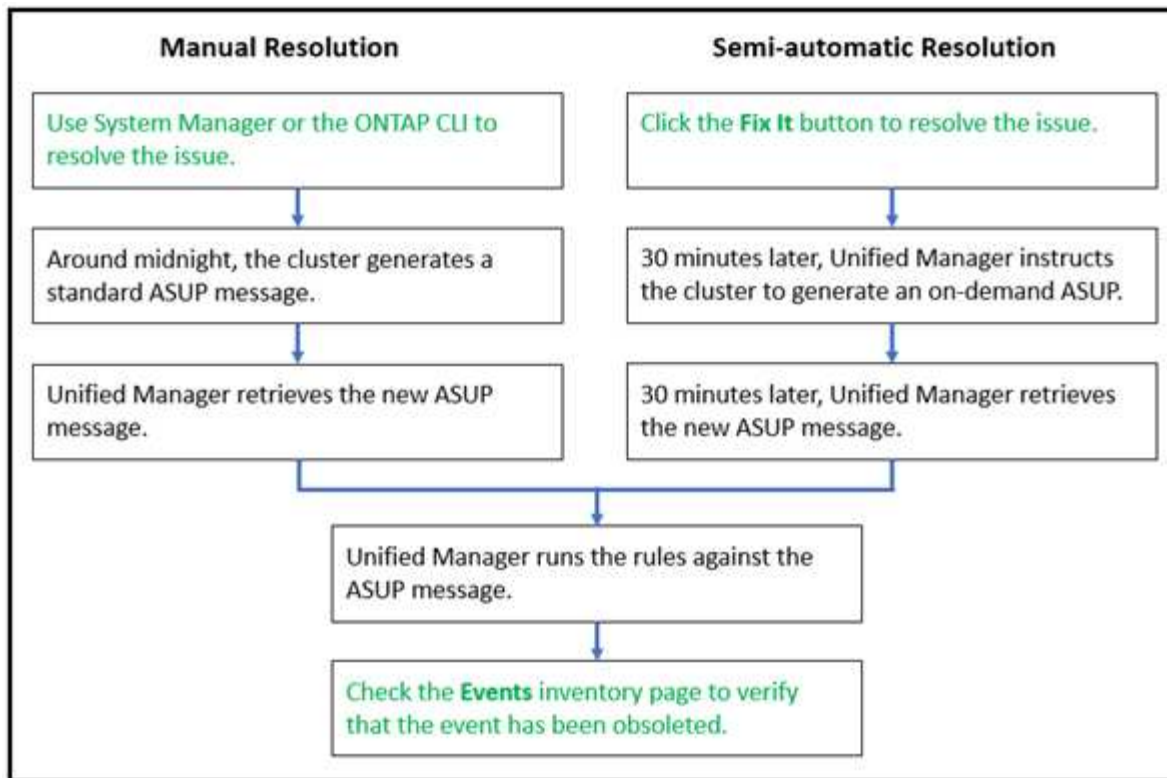


Como você pode ver, o arquivo de regras compilado na plataforma Active IQ é mantido atualizado, as mensagens do AutoSupport do cluster são geradas diariamente e o Unified Manager atualiza a lista de eventos diariamente.

Resolver eventos da plataforma Active IQ

Os incidentes e riscos da plataforma Active IQ são semelhantes a outros eventos do Unified Manager porque podem ser atribuídos a outros usuários para resolução e têm os mesmos estados disponíveis. No entanto, ao resolver esses tipos de eventos usando o botão **Corrigir**, você pode verificar a resolução em poucas horas.

O diagrama a seguir mostra as ações que você deve tomar (em verde) e a ação que o Unified Manager toma (em preto) ao resolver eventos gerados pela plataforma Active IQ.



Ao executar uma resolução manual, você deve fazer login no Gerenciador do Sistema ou na interface de linha de comando do ONTAP para corrigir o problema. Você poderá verificar o problema somente depois que o cluster gerar uma nova mensagem de AutoSupport à meia-noite.

Ao executar uma resolução semiautomática usando o botão **Corrigir**, você pode verificar se a correção foi bem-sucedida em poucas horas.

Configurar definições de retenção de eventos

Você pode especificar o número de meses que um evento será mantido no servidor do Unified Manager antes de ser excluído automaticamente.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Manter eventos por mais de 6 meses pode afetar o desempenho do servidor e não é recomendado.

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 retidos e clique em **Salvar**.

O que é uma janela de manutenção do Unified Manager

Defina uma janela de manutenção do Unified Manager para suprimir eventos e alertas por um período específico quando você tiver agendado manutenção de cluster e não quiser receber uma enxurrada de notificações indesejadas.

Quando a janela de manutenção é iniciada, um evento "Janela de manutenção de objeto iniciada" é publicado na página de inventário do Gerenciamento de eventos. Este evento se torna obsoleto automaticamente quando a janela de manutenção termina.

Durante uma janela de manutenção, os eventos relacionados a todos os objetos naquele cluster ainda são gerados, mas não aparecem em nenhuma das páginas da interface do usuário, e nenhum alerta ou outro tipo de notificação é enviado para esses eventos. No entanto, você pode visualizar 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 do Gerenciamento de Eventos.

Você pode agendar uma janela de manutenção para ser iniciada no futuro, alterar os horários de início e término de uma janela de manutenção agendada e cancelar uma janela de manutenção agendada.

Agende uma janela de manutenção para desabilitar 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

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Durante uma janela de manutenção, os eventos relacionados a todos os objetos naquele cluster ainda são gerados, mas não aparecem na página de eventos, e nenhum alerta ou outro tipo de notificação é enviado para esses eventos.

O horário inserido para a janela de manutenção é baseado no horário no servidor do Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de cluster**.
2. Na coluna **Modo de manutenção** do cluster, selecione o botão deslizante e mova-o para a direita.

A janela do calendário é exibida.

3. Selecione a data e hora de início e término para a janela de manutenção e clique em **Aplicar**.

A mensagem "Agendado" aparece ao lado do botão deslizante.

Quando o horário de início é atingido, o cluster entra no modo de manutenção e um evento "Janela de manutenção de objeto iniciada" é gerado.

Alterar ou cancelar uma janela de manutenção programada

Se você configurou uma janela de manutenção do Unified Manager para ocorrer no futuro, poderá alterar os horários de início e término ou cancelar a ocorrência da janela de manutenção.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Cancelar uma janela de manutenção em execução é útil se você tiver concluído a manutenção do cluster antes do horário de término da janela de manutenção agendada e quiser começar a receber eventos e alertas do cluster novamente.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de cluster**.
2. Na coluna **Modo de manutenção** do cluster:

Se você quiser...	Execute esta etapa...
Alterar o período para uma janela de manutenção programada	a. Clique no texto "Agendado" ao lado do botão deslizante. b. Altere a data e hora de início e/ou término e clique em Aplicar.
Prolongue a duração de uma janela de manutenção ativa	a. Clique no texto "Ativo" ao lado do botão deslizante. b. Altere a data e hora de término e clique em Aplicar.
Cancelar uma janela de manutenção programada	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.

Ver eventos que ocorreram durante uma janela de manutenção

Se necessário, você pode visualizar 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 quando a janela de manutenção for concluída e todos os recursos do sistema estiverem funcionando novamente.

Antes de começar

Pelo menos uma janela de manutenção deve ser concluída antes que qualquer evento esteja disponível.

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 acionados durante os últimos 7 dias de todas as sessões da 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 **Tempo de acionamento** e selecionar o período de tempo para os eventos da janela de manutenção que você deseja visualizar.

Gerenciar eventos de recursos do sistema host

O Unified Manager inclui um serviço que monitora problemas de recursos no sistema host no qual o Unified Manager está instalado. Problemas como falta de espaço em disco disponível 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 insuficiente no sistema host; o Unified Manager não realiza um ciclo regular de coleta de dados; e não conclusão ou conclusão tardia da análise de estatísticas porque a próxima pesquisa de coleta foi iniciada.

Diferentemente de todas as outras mensagens de eventos do Unified Manager, esses eventos críticos e de aviso específicos da estação de gerenciamento são exibidos em mensagens de banner.

Etapas

1. Para visualizar informações sobre eventos da estação de gerenciamento, execute estas ações:

Se você quiser...	Faça isso...
Ver detalhes do evento	Clique no banner do evento para exibir a página de detalhes do evento que inclui soluções sugeridas para o problema.
Ver todos os eventos da estação de gerenciamento	a. No painel de navegação esquerdo, clique em Gerenciamento de eventos. b. No painel Filtros na página de inventário do Gerenciamento de Eventos, clique na caixa Estação de Gerenciamento na lista Tipo de Fonte.

Entenda mais sobre os eventos

Entender os conceitos sobre eventos ajuda você a gerenciar seus clusters e objetos de cluster com eficiência e a definir alertas adequadamente.

Definições de estado de evento

O estado de um evento ajuda a identificar se uma ação corretiva apropriada é necessária. Um evento pode ser Novo, Reconhecido, Resolvido ou Obsoleto. Observe que eventos novos e confirmados 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 reconhece.

- **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.



Você não pode reconhecer ou resolver um evento obsoleto.

Exemplo de diferentes estados de um evento

Os exemplos a seguir ilustram as alterações manuais e automáticas do estado do evento.

Quando o evento Cluster Not Reachable é acionado, o estado do evento é Novo. Quando você reconhece o evento, o estado do evento muda para Reconhecido. Quando você tiver tomado uma ação corretiva apropriada, você deve marcar o evento como resolvido. O estado do evento então muda para Resolvido.

Se o evento Cluster não acessível for gerado devido a uma queda de energia, quando a energia for restaurada, o cluster começará 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. O assunto e o conteúdo do e-mail 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 ajudar você a priorizar os eventos que exigem ação corretiva imediata.

- **Crítico**

Ocorreu um problema que pode levar à interrupção do serviço se uma ação corretiva não for tomada imediatamente.

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

- **Erro**

A origem do evento ainda está em execução; no entanto, uma ação corretiva é necessária para evitar a interrupção do serviço.

- **Aviso**

A origem do evento sofreu uma ocorrência da qual você deve estar ciente, ou um contador de desempenho de um objeto de cluster está fora da faixa normal e deve ser monitorado para garantir que não atinja a gravidade crítica. Eventos dessa gravidade não causam interrupção do serviço e pode não ser necessária ação corretiva imediata.

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 alguma alteração de configuração, o evento com tipo de gravidade Informação é gerado.

Eventos de informação são enviados diretamente do ONTAP quando ele detecta uma alteração de configuração.

Descrição dos níveis de impacto do evento

Cada evento está associado a um nível de impacto (incidente, risco, evento ou atualização) para ajudar você 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. Eventos com nível de impacto Incidente são os mais graves. Medidas corretivas imediatas devem ser tomadas para evitar interrupção do serviço.

- **Risco**

Um risco 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. Eventos com nível de impacto de Risco podem causar interrupção do serviço. Pode ser necessária uma ação corretiva.

- **Evento**

Um evento é uma mudança de estado ou status de objetos de armazenamento e seus atributos. Eventos com nível de impacto Evento são informativos e não exigem ação corretiva.

- **Atualizar**

Eventos de atualização são um tipo específico de evento relatado pela plataforma Active IQ . Esses eventos identificam problemas cuja resolução exige que você atualize o software ONTAP , o firmware do nó ou o software do sistema operacional (para avisos de segurança). Talvez você queira executar ações corretivas imediatas para alguns desses problemas, enquanto outros podem esperar até a próxima manutenção programada.

Descrição das áreas de impacto do evento

Os eventos são categorizados em seis áreas de impacto (disponibilidade, capacidade, configuração, desempenho, proteção e segurança) para permitir que você se concentre nos tipos de eventos pelos quais você é responsável.

- **Disponibilidade**

Os eventos de disponibilidade notificam você 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 seus agregados, volumes, LUNs ou namespaces estão se aproximando ou atingiram um limite de tamanho, ou se a taxa de crescimento é incomum para 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 impacto de Evento e um tipo de gravidade de Informação.

- **Desempenho**

Os eventos de desempenho notificam você sobre condições de recursos, configuração ou atividade no seu cluster que podem afetar negativamente a velocidade de entrada ou recuperação de armazenamento de dados nos seus objetos de armazenamento monitorados.

- **Proteção**

Os eventos de proteção notificam você sobre incidentes ou riscos envolvendo relacionamentos do SnapMirror , problemas com capacidade de destino, problemas com relacionamentos do SnapVault ou problemas com trabalhos de proteção. Qualquer objeto ONTAP (especialmente agregados, volumes e SVMs) que hospeda volumes secundários e relacionamentos de proteção é categorizado na área de impacto de proteção.

- **Segurança**

Os eventos de segurança notificam você sobre a segurança dos seus clusters ONTAP , máquinas virtuais de armazenamento (SVMs) e volumes com base em parâmetros definidos no ["Guia de reforço de segurança da NetApp para ONTAP 9"](#) .

Além disso, esta área inclui eventos de atualização que são relatados pela 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 o status de um objeto for Erro, um dos eventos do objeto terá um tipo de gravidade Erro. Quando uma ação corretiva for tomada, o estado do evento mudará para Resolvido.

Detalhes do gráfico de eventos de desempenho dinâmico

Para eventos de desempenho dinâmico, a seção Diagnóstico do Sistema da página Detalhes do Evento lista as principais cargas de trabalho com maior latência ou uso do componente do cluster que está em contenção.

As estatísticas de desempenho são baseadas no momento em que o evento de desempenho foi detectado até a última vez que o evento foi analisado. Os gráficos também exibem estatísticas históricas de desempenho para o componente do cluster que está na disputa.

Por exemplo, você pode identificar cargas de trabalho com alta utilização de um componente para determinar qual carga de trabalho mover para um componente menos utilizado. Mover a carga de trabalho reduziria a quantidade de trabalho no componente atual, possivelmente tirando o componente da disputa. No topo desta seção está o intervalo de data e hora em que um evento foi detectado e analisado pela última vez. Para eventos ativos (novos ou reconhecidos), o último horário analisado é atualizado.

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 *tubarões*, *valentões* ou *vítimas*, e exibe detalhes sobre sua latência e seu uso no componente do cluster em contenção. Você pode comparar o valor real com o valor esperado para ver quando a carga de trabalho estava fora do intervalo esperado de latência ou uso. Para obter informações, consulte "[Tipos de cargas de trabalho monitoradas pelo Unified Manager](#)".



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 às cargas de trabalho definidas pelo usuário. Cargas de trabalho com valores de latência muito baixos não são exibidas na tabela.

Para obter mais informações sobre os limites de desempenho dinâmico, consulte "[Analisando eventos a partir de limites de desempenho dinâmico](#)".

Para obter informações sobre como o Unified Manager classifica as cargas de trabalho e determina a ordem de classificação, consulte "[Como o Unified Manager determina o impacto no desempenho de um evento](#)".

Os dados nos gráficos mostram 24 horas de estatísticas de desempenho anteriores à última vez que o evento foi analisado. Os valores reais e esperados para cada carga de trabalho são baseados no tempo em que a carga de trabalho esteve envolvida no evento. Por exemplo, uma carga de trabalho pode se envolver em um evento depois que ele foi detectado, de modo que suas estatísticas de desempenho podem não corresponder aos valores no momento da detecção do evento. Por padrão, as cargas de trabalho são classificadas por pico (maior) desvio na latência.



Como o Unified Manager retém no máximo 30 dias de dados históricos de desempenho e eventos de 5 minutos, se o evento tiver mais de 30 dias, nenhum dado de desempenho será exibido.

• Coluna de classificação de carga de trabalho

◦ Gráfico de latência

Exibe o impacto do evento na latência da carga de trabalho durante a última análise.

◦ Coluna de Uso de Componentes

Exibe detalhes sobre o uso da carga de trabalho do componente do cluster em contenção. Nos gráficos, o uso real é uma linha azul. Uma barra vermelha destaca a duração do evento, desde o momento da detecção até o último momento analisado. Para mais informações, consulte "[Valores de medição de desempenho da carga de trabalho](#)".



Para o componente de rede, como as estatísticas de desempenho da rede vêm da atividade fora do cluster, esta coluna não é exibida.

- **Uso de componentes**

Exibe o histórico de utilização, em porcentagem, para os componentes de processamento de rede, processamento de dados e agregados ou o histórico de atividade, em porcentagem, para o componente de grupo de política 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 momento específico.

- **Histórico total de MB/s de gravação**

Somente para o componente Recursos do MetroCluster, mostra a taxa de transferência total de gravação, em megabytes por segundo (MBps), para todas as cargas de trabalho de volume que estão sendo espelhadas para o cluster parceiro em uma configuração do MetroCluster.

- **Histórico do Evento**

Exibe linhas sombreadas em vermelho para indicar os eventos históricos do componente em disputa. Para eventos obsoletos, o gráfico exibe eventos que ocorreram antes do evento selecionado ser detectado e depois que ele foi resolvido.

Alterações de configuração detectadas pelo Unified Manager

O Unified Manager monitora seus clusters em busca de alterações de configuração para ajudar você a determinar se uma alteração pode ter causado ou contribuído para um evento de desempenho. As páginas do Performance Explorer exibem um ícone de evento de alteração () para indicar a data e a hora em que a alteração foi detectada.

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 alteração impactou o desempenho do objeto de cluster selecionado. Se a alteração foi detectada no mesmo momento ou próximo a um evento de desempenho, a alteração pode ter contribuído para o problema, o que fez com que o alerta do evento fosse acionado.

O Unified Manager pode detectar os seguintes eventos de alteração, que são categorizados como eventos informativos:

- Um volume se move entre agregados.

O Unified Manager pode detectar quando a movimentação está em andamento, concluída ou falhou. Se o Unified Manager estiver inativo durante uma movimentação de volume, quando ele voltar a funcionar, ele detectará a movimentação de volume e exibirá um evento de alteração para ela.

- O limite de taxa de transferência (MB/s ou IOPS) de um grupo de políticas de QoS que contém uma ou mais cargas de trabalho monitoradas muda.

Alterar um limite de 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 retorna gradualmente ao normal e quaisquer eventos causados pelos picos se tornam obsoletos.

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

O Unified Manager pode detectar quando a operação de aquisição, aquisição parcial ou devolução foi concluída. Se a aquisição for causada por um nó em pânico, o Unified Manager não detectará o evento.

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

A versão anterior e a nova versão são exibidas.

Lista de eventos e tipos de gravidade

Você pode usar a lista de eventos para se familiarizar mais com as categorias de eventos, os nomes dos 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.

Eventos agregados

Os eventos agregados fornecem informações sobre o status dos agregados para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: disponibilidade

Um asterisco (*) identifica eventos do EMS que foram convertidos em eventos do Unified Manager.

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Agregar Offline(ocumEvtAggregateStateOffline)	Incidente	Agregar	Crítico
Falha na agregação (ocumEvtAggregateStateFailed)	Incidente	Agregar	Crítico
Agregado restrito (ocumEvtAggregateStateRestricted)	Risco	Agregar	Aviso
Reconstrução de Agregados (ocumEvtAggregateRaidStateReconstructing)	Risco	Agregar	Aviso
Agregado Degradado (ocumEvtAggregateRaidStateDegraded)	Risco	Agregar	Aviso
Camada de nuvem parcialmente acessível (ocumEventCloudTierPartiallyReachable)	Risco	Agregar	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Camada de nuvem inacessível (ocumEventCloudTierUnreachable)	Risco	Agregar	Erro
Acesso à camada de nuvem negado para realocação agregada (arlNetraCaCheckFailed)	Risco	Agregar	Erro
Acesso à camada de nuvem negado para realocação agregada durante failover de armazenamento (gbNetraCaCheckFailed)	Risco	Agregar	Erro
Agregado do MetroCluster deixado para trás (ocumEvtMetroClusterAggregateLeftBehind)	Risco	Agregar	Erro
Espelhamento de agregados do MetroCluster degradado (ocumEvtMetroClusterAggregateMirrorDegraded)	Risco	Agregar	Erro

Área de impacto: capacidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Espaço agregado quase cheio (ocumEvtAggregateNearlyFull)	Risco	Agregar	Aviso
Espaço agregado completo (ocumEvtAggregateFull)	Risco	Agregar	Erro
Dias agregados até a conclusão (ocumEvtAggregateDaysUntilFullSoon)	Risco	Agregar	Erro

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Agregado Supercomprometido (ocumEvtAggregateOvercommitted)	Risco	Agregar	Erro
Agregado quase supercomprometido (ocumEvtAggregateAlmostOvercommitted)	Risco	Agregar	Aviso
Reserva de instantâneo agregado completa (ocumEvtAggregateSnapshotReserveFull)	Risco	Agregar	Aviso
Taxa de crescimento agregada anormal (ocumEvtAggregateGrowthRateAbnormal)	Risco	Agregar	Aviso

Área de impacto: configuração

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Agregado descoberto (não aplicável)	Evento	Agregar	Informação
Agregado renomeado (não aplicável)	Evento	Agregar	Informação
Agregado excluído (não aplicável)	Evento	Nó	Informação

Área de impacto: desempenho

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Límite crítico de IOPS agregado violado (ocumAggregateIopsIncident)	Incidente	Agregar	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite de aviso de IOPS agregado violado (ocumAggregateIopsWarning)	Risco	Agregar	Aviso
Limite crítico de MB/s agregado violado (ocumAggregateMbpsIncident)	Incidente	Agregar	Crítico
Limite de alerta de MB/s agregado violado (ocumAggregateMbpsWarning)	Risco	Agregar	Aviso
Limite crítico de latência agregada violado (ocumAggregateLatencyIncident)	Incidente	Agregar	Crítico
Limite de aviso de latência agregada violado (ocumAggregateLatencyWarning)	Risco	Agregar	Aviso
Limite crítico de capacidade de desempenho agregado violado (ocumAggregatePerfCapacityUsedIncident)	Incidente	Agregar	Crítico
Limite de aviso de capacidade de desempenho agregada usada violado (ocumAggregatePerfCapacityUsedWarning)	Risco	Agregar	Aviso
Limite crítico de utilização agregada violado (ocumAggregateUtilizationIncident)	Incidente	Agregar	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite de aviso de utilização agregada violado (ocumAggregateUtilizationWarning)	Risco	Agregar	Aviso
Limite de superutilização de discos agregados violado (ocumAggregateDisksOverUtilizedWarning)	Risco	Agregar	Aviso
Limite dinâmico agregado violado (ocumAggregateDynamicEventWarning)	Risco	Agregar	Aviso

Eventos de cluster

Os eventos de 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 impacto e incluem o nome do evento, o nome da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Área de impacto: disponibilidade

Um asterisco (*) identifica eventos do EMS que foram convertidos em eventos do Unified Manager.

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
O cluster não possui discos sobressalentes (ocumEvtDisksNoSpares)	Risco	Conjunto	Aviso
Cluster não alcançável (ocumEvtClusterUnreachable)	Risco	Conjunto	Erro
Falha no monitoramento de cluster (ocumEvtClusterMonitoringFailed)	Risco	Conjunto	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limites de capacidade da licença do Cluster FabricPool violados (ocumEvtExternalCapacityTierSpaceFull)	Risco	Conjunto	Aviso
Período de carência NVMe-oF iniciado *(nvmfGracePeriodStart)	Risco	Conjunto	Aviso
Período de carência NVMe-oF ativo *(nvmfGracePeriodActive)	Risco	Conjunto	Aviso
Período de carência NVMe-oF expirado *(nvmfGracePeriodExpired)	Risco	Conjunto	Aviso
Janela de manutenção de objeto iniciada (objectMaintenanceWindowStarted)	Evento	Conjunto	Crítico
Janela de manutenção de objeto encerrada (objectMaintenanceWindowEnded)	Evento	Conjunto	Informação
Discos sobressalentes do MetroCluster deixados para trás (ocumEvtSpareDiskLeftBehind)	Risco	Conjunto	Erro
Comutação automática não planejada do MetroCluster desabilitada (ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Risco	Conjunto	Aviso
Senha do usuário do cluster alterada *(cluster.passwd.changed)	Evento	Conjunto	Informação

Área de impacto: capacidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite de desequilíbrio de capacidade do cluster violado (ocumConformanceNodeImbalanceWarning)	Risco	Conjunto	Aviso
Planejamento da camada de nuvem do cluster (clusterCloudTierPlanningWarning)	Risco	Conjunto	Aviso
Ressincronização de replicação do espelho do FabricPool concluída (wafCaResyncComplete)	Evento	Conjunto	Aviso
Espaço do FabricPool quase cheio (fabricpoolNearlyFull)	Risco	Conjunto	Erro

Área de impacto: configuração

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Nó adicionado (não aplicável)	Evento	Conjunto	Informação
Nó removido (não aplicável)	Evento	Conjunto	Informação
Cluster removido (não aplicável)	Evento	Conjunto	Informação
Falha ao adicionar cluster (não aplicável)	Evento	Conjunto	Erro
Nome do cluster alterado (não aplicável)	Evento	Conjunto	Informação
EMS de emergência recebido (não aplicável)	Evento	Conjunto	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
EMS crítico recebido (não aplicável)	Evento	Conjunto	Crítico
Alerta EMS recebido (Não aplicável)	Evento	Conjunto	Erro
Erro EMS recebido (Não aplicável)	Evento	Conjunto	Aviso
Aviso EMS recebido (Não aplicável)	Evento	Conjunto	Aviso
Depurar EMS recebido (Não aplicável)	Evento	Conjunto	Aviso
Aviso EMS recebido (Não aplicável)	Evento	Conjunto	Aviso
EMS informativo recebido (Não aplicável)	Evento	Conjunto	Aviso

Os eventos do ONTAP EMS são categorizados em três níveis de gravidade de eventos do Unified Manager.

Nível de gravidade do evento do Unified Manager	Nível de gravidade do evento ONTAP EMS
Crítico	Emergência Crítico
Erro	Alerta
Aviso	Erro Aviso Depurar Perceber Informativo

Área de impacto: desempenho

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite de desequilíbrio de carga do cluster violado()	Risco	Conjunto	Aviso
Limite crítico de IOPS do cluster violado (ocumClusterIopsIncident)	Incidente	Conjunto	Crítico
Limite de aviso de IOPS de cluster violado (ocumClusterIopsWarning)	Risco	Conjunto	Aviso
Limite crítico de MB/s do cluster violado (ocumClusterMbpsIncident)	Incidente	Conjunto	Crítico
Limite de alerta de cluster MB/s violado (ocumClusterMbpsWarning)	Risco	Conjunto	Aviso
Limite dinâmico do cluster violado (ocumClusterDynamicEventWarning)	Risco	Conjunto	Aviso

Área de impacto: segurança

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Transporte HTTPS de AutoSupport desabilitado (ocumClusterASUPHttpsConfiguredDisabled)	Risco	Conjunto	Aviso
Encaminhamento de log não criptografado (ocumClusterAuditLogUnencrypted)	Risco	Conjunto	Aviso
Usuário administrador local padrão habilitado (ocumClusterDefaultAdminEnabled)	Risco	Conjunto	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Modo FIPS desabilitado (ocumClusterFipsDisabled)	Risco	Conjunto	Aviso
Banner de login desabilitado (ocumClusterLoginBannerDisabled)	Risco	Conjunto	Aviso
Banner de login alterado (ocumClusterLoginBannerChanged)	Risco	Conjunto	Aviso
Destinos de encaminhamento de log alterados (ocumLogForwardDestinationsChanged)	Risco	Conjunto	Aviso
Nomes de servidores NTP alterados (ocumNtpServerNamesChanged)	Risco	Conjunto	Aviso
A contagem do servidor NTP está baixa (securityConfigNTPServerCountLowRisk)	Risco	Conjunto	Aviso
Comunicação entre pares do cluster não criptografada (ocumClusterPeerEncryptionDisabled)	Risco	Conjunto	Aviso
SSH está usando cifras inseguras (ocumClusterSSHInsecure)	Risco	Conjunto	Aviso
Protocolo Telnet habilitado (ocumClusterTelnetEnabled)	Risco	Conjunto	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
As senhas de algumas contas de usuários do ONTAP usam a função de hash MD5 menos segura (ocumClusterMD5PasswordHashUsed)	Risco	Conjunto	Aviso
O cluster usa certificado autoassinado (ocumClusterSelfSignedCertificate)	Risco	Conjunto	Aviso
O Cluster Remote Shell está habilitado (ocumClusterRshDisabled)	Risco	Conjunto	Aviso
Certificado de cluster prestes a expirar (ocumEvtClusterCertificateAboutToExpire)	Risco	Conjunto	Aviso
Certificado de cluster expirado (ocumEvtClusterCertificateExpired)	Risco	Conjunto	Erro

Eventos de discos

Os eventos de discos fornecem informações sobre o status dos discos para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Discos Flash - Blocos Sobressalentes Quase Consumidos (ocumEvtClusterFlashDiskFewerSpareBlockError)	Risco	Conjunto	Erro

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Discos Flash - Sem Blocos Sobressalentes (ocumEvtClusterFlashDiskNoSpareBlockCritical)	Incidente	Conjunto	Crítico
Alguns discos não atribuídos (ocumEvtClusterUnassignedDisksSome)	Risco	Conjunto	Aviso
Alguns discos com falha (ocumEvtDisksSomeFailed)	Incidente	Conjunto	Crítico

Eventos de recintos

Os eventos de gabinetes fornecem informações sobre o status dos gabinetes de prateleira de disco no seu data center para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Falha nos ventiladores da prateleira de disco (ocumEvtShelfFanFailed)	Incidente	Prateleira de armazenamento	Crítico
Falha nas fontes de alimentação da prateleira de disco (ocumEvtShelfPowerSupplyFailed)	Incidente	Prateleira de armazenamento	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Multicaminho da prateleira de disco não configurado (ocumDiskShelfConnectivityNotInMultiPath) Este evento não se aplica a: - Clusters que estão em uma configuração MetroCluster - As seguintes plataformas: FAS2554, FAS2552, FAS2520 e FAS2240	Risco	Nó	Aviso
Falha no caminho da prateleira de disco (ocumDiskShelfConnectivityPathFailure)	Risco	Prateleira de armazenamento	Aviso

Área de impacto: configuração

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Prateleira de disco descoberta (não aplicável)	Evento	Nó	Informação
Prateleiras de disco removidas (não aplicável)	Evento	Nó	Informação

Eventos para fãs

Os eventos de fãs fornecem informações sobre o status dos fãs nos nós do seu data center para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Um ou mais fãs com falha (ocumEvtFansOneOrMoreFailed)	Incidente	Nó	Crítico

Eventos de flashcards

Os eventos de flash cards fornecem informações sobre o status dos flash cards instalados nos nós do seu data center para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Flashcards offline (ocumEvtFlashCardOffline)	Incidente	Nó	Crítico

Eventos de inodes

Os eventos de 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 impacto e incluem o nome do evento e da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Área de impacto: capacidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Inodes quase cheios (ocumEvtInodesAlmostFull)	Risco	Volume	Aviso
Inodes completos (ocumEvtInodesFull)	Risco	Volume	Erro

Eventos de interface de rede (LIF)

Os eventos da interface de rede fornecem informações sobre o status da sua interface de rede (LIFs), para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Status da interface de rede inativo (ocumEvtLifStatusDown)	Risco	Interface	Erro
Status da interface de rede FC/FCoE inativo (ocumEvtFCLifStatusDown)	Risco	Interface	Erro
Failover de interface de rede não é possível (ocumEvtLifFailoverNotPossible)	Risco	Interface	Aviso
Interface de rede não está na porta doméstica (ocumEvtLifNotAtHomePort)	Risco	Interface	Aviso

Área de impacto: configuração

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Rota da interface de rede não configurada (não aplicável)	Evento	Interface	Informação

Área de impacto: desempenho

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de MB/s da interface de rede violado (ocumNetworkLifMbpsIncident)	Incidente	Interface	Crítico
Limite de alerta de MB/s da interface de rede violado (ocumNetworkLifMbpsWarning)	Risco	Interface	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de MB/s da interface de rede FC violado (ocumFcpLifMbpsIncident)	Incidente	Interface	Crítico
Limite de alerta de MB/s da interface de rede FC violado (ocumFcpLifMbpsWarning)	Risco	Interface	Aviso
Limite crítico MB/s da interface de rede NVMf FC violado (ocumNvmfFcLifMbpsIncident)	Incidente	Interface	Crítico
Limite de alerta de MB/s da interface de rede NVMf FC violado (ocumNvmfFcLifMbpsWarning)	Risco	Interface	Aviso

Eventos LUN

Os eventos de LUN fornecem informações sobre o status dos seus LUNs, para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Área de impacto: disponibilidade

Um asterisco (*) identifica eventos do EMS que foram convertidos em eventos do Unified Manager.

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
LUN offline (ocumEvtLunOffline)	Incidente	LUN	Crítico
LUN destruído *(lunDestroy)	Evento	LUN	Informação

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
LUN mapeado com sistema operacional não suportado no igroup(igroupUnsupportedOsType)	Incidente	LUN	Aviso
Caminho ativo único para acessar LUN (ocumEvtLunSingleActivePath)	Risco	LUN	Aviso
Nenhum caminho ativo para acessar LUN (ocumEvtLunNotReachable)	Incidente	LUN	Crítico
Nenhum caminho otimizado para acessar o LUN (ocumEvtLunOptimizedPathInactive)	Risco	LUN	Aviso
Nenhum caminho para acessar o LUN do parceiro HA (ocumEvtLunHaPathInactive)	Risco	LUN	Aviso
Nenhum caminho para acessar o LUN de um nó no par HA (ocumEvtLunNodePathStatusDown)	Risco	LUN	Erro

Área de impacto: capacidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Espaço insuficiente para cópia de instantâneo de LUN (ocumEvtLunSnapshotNotPossible)	Risco	Volume	Aviso

Área de impacto: configuração

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
LUN mapeado com sistema operacional não suportado no igroup(igroupUnsupportedOsType)	Risco	LUN	Aviso

Área de impacto: desempenho

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de IOPS de LUN violado (ocumLunIopsIncident)	Incidente	LUN	Crítico
Limite de aviso de IOPS de LUN violado (ocumLunIopsWarning)	Risco	LUN	Aviso
Limite crítico de LUN MB/s violado (ocumLunMbpsIncident)	Incidente	LUN	Crítico
Limite de alerta de LUN MB/s violado (ocumLunMbpsWarning)	Risco	LUN	Aviso
Limite crítico de latência de LUN ms/op violado (ocumLunLatencyIncident)	Incidente	LUN	Crítico
Limite de alerta de latência de LUN ms/op violado (ocumLunLatencyWarning)	Risco	LUN	Aviso
Limite crítico de latência de LUN e IOPS violado (ocumLunLatencyIopsIncident)	Incidente	LUN	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite de alerta de latência de LUN e IOPS violado (ocumLunLatencyIopsWarning)	Risco	LUN	Aviso
Limite crítico de latência de LUN e MB/s violado (ocumLunLatencyMbpsIncident)	Incidente	LUN	Crítico
Limite de alerta de latência de LUN e MB/s violado (ocumLunLatencyMbpsWarning)	Risco	LUN	Aviso
Limite crítico de latência de LUN e capacidade de desempenho agregado violado (ocumLunLatencyAggregatePerfCapacityUsedIncident)	Incidente	LUN	Crítico
Limite de aviso de latência de LUN e capacidade de desempenho agregado usada violado (ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risco	LUN	Aviso
Limite crítico de latência de LUN e utilização agregada violado (ocumLunLatencyAggregateUtilizationIncident)	Incidente	LUN	Crítico
Limite de aviso de latência de LUN e utilização agregada violado (ocumLunLatencyAggregateUtilizationWarning)	Risco	LUN	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de latência de LUN e capacidade de desempenho de nó violado (ocumLunLatencyNodePerfCapacityUsedIncident)	Incidente	LUN	Crítico
Limite de aviso de capacidade usada de desempenho do nó e latência do LUN violado (ocumLunLatencyNodePerfCapacityUsedWarning)	Risco	LUN	Aviso
Latência de LUN e capacidade de desempenho do nó usada - Limite crítico de aquisição violado (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incidente	LUN	Crítico
Latência de LUN e capacidade de desempenho do nó usada - Limite de aviso de aquisição violado (ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risco	LUN	Aviso
Limite crítico de latência de LUN e utilização de nó violado (ocumLunLatencyNodeUtilizationIncident)	Incidente	LUN	Crítico
Limite de aviso de latência de LUN e utilização de nó violado (ocumLunLatencyNodeUtilizationWarning)	Risco	LUN	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite de aviso de IOPS máximo de QoS LUN violado (ocumQosLunMaxIopsWarning)	Risco	LUN	Aviso
Limite de alerta de QoS LUN Max MB/s violado (ocumQosLunMaxMbpsWarning)	Risco	LUN	Aviso
Limite de latência do 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 impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: configuração

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Espaço em disco do servidor de gerenciamento quase cheio (ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Risco	Estação de gerenciamento	Aviso
Espaço em disco do servidor de gerenciamento cheio (ocumEvtUnifiedManagerDiskSpaceFull)	Incidente	Estação de gerenciamento	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Servidor de gerenciamento com pouca memória (ocumEvtUnifiedManagerMemoryLow)	Risco	Estação de gerenciamento	Aviso
Servidor de gerenciamento quase sem memória (ocumEvtUnifiedManagerMemoryAlmostOut)	Incidente	Estação de gerenciamento	Crítico
Tamanho do arquivo de log do MySQL aumentado; reinicialização necessária (ocumEvtMysqlLogFileSizeWarning)	Incidente	Estação de gerenciamento	Aviso
A alocação total do tamanho do log de auditoria está prestes a ficar cheia	Risco	Estação de gerenciamento	Aviso
Certificado do servidor Syslog prestes a expirar	Risco	Estação de gerenciamento	Aviso
Certificado do servidor Syslog expirado	Risco	Estação de gerenciamento	Erro
Arquivo de log de auditoria adulterado	Risco	Estação de gerenciamento	Aviso
Arquivo de log de auditoria excluído	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 impacto: desempenho

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
A análise de dados de desempenho é impactada (ocumEvtUnifiedManagerDataMissingAnalyze)	Risco	Estação de gerenciamento	Aviso
A coleta de dados de desempenho foi impactada (ocumEvtUnifiedManagerDataMissingCollection)	Incidente	Estação de gerenciamento	Crítico



Esses dois últimos eventos de desempenho estavam disponíveis apenas para o Unified Manager 7.2. Se qualquer um desses eventos existir no estado Novo e 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.

Eventos da Ponte MetroCluster

Os eventos do MetroCluster Bridge fornecem informações sobre o status das bridges para que você possa monitorar possíveis problemas em uma configuração do MetroCluster sobre FC. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Ponte inalcançável (ocumEvtBridgeUnreachable)	Incidente	Ponte MetroCluster	Crítico
Temperatura da ponte anormal (ocumEvtBridgeTemperatureAbnormal)	Incidente	Ponte MetroCluster	Crítico

Eventos de conectividade do 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 possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Eventos comuns em ambas as configurações

Esses eventos de conectividade são comuns para configurações do MetroCluster sobre FC e do MetroCluster sobre IP.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Todos os links entre os parceiros do MetroCluster estão inativos (ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Incidente	Relação MetroCluster	Crítico
Parceiros do MetroCluster não acessíveis pela rede peering (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Incidente	Relação MetroCluster	Crítico
Capacidade de recuperação de desastres do MetroCluster impactada (ocumEvtMetroClusterDRStatusImpacted)	Risco	Relação MetroCluster	Crítico
Configuração do MetroCluster alterada (ocumEvtMetroClusterDRStatusImpacted)	Risco	Relação MetroCluster	Aviso

Configuração do MetroCluster sobre FC

Esses eventos pertencem ao MetroCluster sobre configurações de FC.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Todos os links entre switches estão inativos (ocumEvtMetroClusterAllSLBetweenSwitchesDown)	Incidente	Conexão entre switches do MetroCluster	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Ponte FC-SAS para link de pilha de armazenamento inativo (ocumEvtBridgeSasPortDown)	Incidente	Conexão de pilha de ponte MetroCluster	Crítico
Configuração do MetroCluster parcialmente alterada (ocumEvtMetroClusterDRStatusPartiallyImpacted)	Risco	Relação MetroCluster	Erro
Nó para FC Switch Todos os links de interconexão FC-VI desativados (ocumEvtMccNodeSwitchFcviLinksDown)	Incidente	Conexão do switch do nó MetroCluster	Crítico
Nó para comutador FC com um ou mais links de iniciador FC inativos (ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Risco	Conexão do switch do nó MetroCluster	Aviso
Nó para FC comuta todos os links do iniciador FC inativos (ocumEvtMccNodeSwitchFcLinksDown)	Incidente	Conexão do switch do nó MetroCluster	Crítico
Alternar para a ponte FC-SAS Link FC inativo (ocumEvtMccSwitchBridgeFcLinksDown)	Incidente	Conexão de ponte de switch MetroCluster	Crítico
Todos os links de interconexão do FC VI entre nós estão inativos (ocumEvtMccInterNodeLinksDown)	Incidente	Conexão entre nós	Crítico
Inter Node Um ou mais links de interconexão FC VI inativos (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risco	Conexão entre nós	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Link de nó para ponte inativo (ocumEvtMccNodeBridgeLinksDown)	Incidente	Conexão de ponte de nó	Crítico
Nó para pilha de armazenamento Todos os links SAS inativos (ocumEvtMccNodeStackLinksDown)	Incidente	Conexão de pilha de nós	Crítico
Nó para pilha de armazenamento com um ou mais links SAS inativos (ocumEvtMccNodeStackLinksOneOrMoreDown)	Risco	Conexão de pilha de nós	Aviso

Configuração do MetroCluster sobre IP

Esses eventos pertencem às configurações do MetroCluster sobre IP.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
O status de conectividade entre sites do MetroCluster IP está inativo (mccIntersiteconnectivityStatusDown)	Risco	Relacionamento MetroCluster	Crítico
MetroCluster- Conexão de nó IP para switch offline (mccIpPortStatusOffline)	Risco	Nó	Erro

Eventos de troca do MetroCluster

Os eventos de switch do MetroCluster para configurações do MetroCluster sobre FC fornecem informações sobre o status dos switches do MetroCluster para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Temperatura do interruptor anormal (ocumEvtSwitchTemperatureAbnormal)	Incidente	Comutador MetroCluster	Crítico
Interruptor inacessível (ocumEvtSwitchUnreachable)	Incidente	Comutador MetroCluster	Crítico
Falha nos ventiladores do switch (ocumEvtSwitchFansOneOrMoreFailed)	Incidente	Comutador MetroCluster	Crítico
Falha nas fontes de alimentação do switch (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Incidente	Comutador MetroCluster	Crítico
 Este evento é aplicável somente para switches Cisco . Falha nos sensores de temperatura do interruptor (ocumEvtSwitchTemperatureSensorFailed)	Incidente	Comutador MetroCluster	Crítico

Eventos de namespace NVMe

Os eventos de namespace NVMe fornecem informações sobre o status dos seus namespaces, para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Um asterisco (*) identifica eventos do EMS que foram convertidos em eventos do Unified Manager.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
NVMeNS Offline *(nvmeNamespaceStatusOffline)	Evento	Espaço de nomes	Informação
NVMeNS Online *(nvmeNamespaceStatusOnline)	Evento	Espaço de nomes	Informação
NVMeNS sem espaço *(nvmeNamespaceSpaceOutOfSpace)	Risco	Espaço de nomes	Aviso
NVMeNS Destruir *(nvmeNamespaceDestroy)	Evento	Espaço de nomes	Informação

Área de impacto: desempenho

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de IOPS do namespace NVMe violado (ocumNvmeNamespaceIopsIncident)	Incidente	Espaço de nomes	Crítico
Limite de aviso de IOPS de namespace NVMe violado (ocumNvmeNamespaceIopsWarning)	Risco	Espaço de nomes	Aviso
Limite crítico de MB/s do namespace NVMe violado (ocumNvmeNamespaceMbpsIncident)	Incidente	Espaço de nomes	Crítico
Limite de aviso de MB/s do namespace NVMe violado (ocumNvmeNamespaceMbpsWarning)	Risco	Espaço de nomes	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de latência de namespace NVMe ms/op violado (ocumNvmeNamespaceLatencyIncident)	Incidente	Espaço de nomes	Crítico
Limite de aviso de latência de namespace NVMe ms/op violado (ocumNvmeNamespaceLatencyWarning)	Risco	Espaço de nomes	Aviso
Limite crítico de latência e IOPS do namespace NVMe violado (ocumNvmeNamespaceLatencyIopsIncident)	Incidente	Espaço de nomes	Crítico
Limite de alerta de latência e IOPS do namespace NVMe violado (ocumNvmeNamespaceLatencyIopsWarning)	Risco	Espaço de nomes	Aviso
Latência do namespace NVMe e limite crítico de MB/s violados (ocumNvmeNamespaceLatencyMbpsIncident)	Incidente	Espaço de nomes	Crítico
Limite de alerta de latência de namespace NVMe e MB/s violado (ocumNvmeNamespaceLatencyMbpsWarning)	Risco	Espaço de nomes	Aviso

Eventos de 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 impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Um asterisco (*) identifica eventos do EMS que foram convertidos em eventos do Unified Manager.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Espaço do volume raiz do nó quase cheio (ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risco	Nó	Aviso
Nuvem AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	Risco	Nó	Erro
Nuvem AWS IAMCredsExpirado *(ocumCloudAwsIamCredsExpired)	Risco	Nó	Erro
Nuvem AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	Risco	Nó	Erro
Nuvem AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	Risco	Nó	Erro
Nuvem AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	Evento	Nó	Informação
Nuvem AWS IAMRoleInválido *(ocumCloudAwsIamRoleInválido)	Risco	Nó	Erro
Nuvem AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	Risco	Nó	Erro
Host da camada de nuvem não resolvível *(ocumObjstoreHostUnresolvable)	Risco	Nó	Erro

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Interface de rede intercluster da camada de nuvem inativa *(ocumObjstoreInterClusterLifDown)	Risco	Nó	Erro
Um dos pools NFSv4 esgotados *(nbladeNfsv4PoolExhaust)	Incidente	Nó	Crítico
Assinatura da camada de nuvem de incompatibilidade de solicitação *(oscSignatureMismatch)	Risco	Nó	Erro

Área de impacto: capacidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Memória do monitor QoS máxima *(ocumQosMonitorMemoryMaxed)	Risco	Nó	Erro
Memória do monitor QoS reduzida *(ocumQosMonitorMemoryAbated)	Evento	Nó	Informação

Área de impacto: configuração

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Nó renomeado (não aplicável)	Evento	Nó	Informação

Área de impacto: desempenho

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de IOPS do nó violado (ocumNodeIopsIncident)	Incidente	Nó	Crítico
Limite de aviso de IOPS de nó violado (ocumNodeIopsWarning)	Risco	Nó	Aviso
Limite crítico de MB/s do nó violado (ocumNodeMbpsIncident)	Incidente	Nó	Crítico
Limite de aviso de MB/s do nó violado (ocumNodeMbpsWarning)	Risco	Nó	Aviso
Limite crítico de latência do nó ms/op violado (ocumNodeLatencyIncident)	Incidente	Nó	Crítico
Limite de alerta de latência do nó ms/op violado (ocumNodeLatencyWarning)	Risco	Nó	Aviso
Limite crítico de capacidade de desempenho do nó violado (ocumNodePerfCapacityUsedIncident)	Incidente	Nó	Crítico
Limite de aviso de capacidade de desempenho do nó violado (ocumNodePerfCapacityUsedWarning)	Risco	Nó	Aviso
Capacidade de desempenho do nó usada - Limite crítico de aquisição violado (ocumNodePerfCapacityUsedTakeoverIncident)	Incidente	Nó	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	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
Limite de superutilização do par de HA do nó violado (ocumNodeHaPairOverUtilizedInformation)	Evento	Nó	Informação
Limite de fragmentação de disco do nó violado (ocumNodeDiskFragmentationWarning)	Risco	Nó	Aviso
Limite de capacidade de desempenho usada violado (ocumNodeOverUtilizedWarning)	Risco	Nó	Aviso
Limite dinâmico do nó violado (ocumNodeDynamicEventWarning)	Risco	Nó	Aviso

Área de impacto: segurança

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
ID do aviso: NTAP- <i><ID do aviso></i> (ocumx)	Risco	Nó	Crítico

Eventos de bateria NVRAM

Os eventos da bateria NVRAM fornecem informações sobre o status das suas baterias para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Bateria NVRAM fraca (ocumEvtNvramBatteryLow)	Risco	Nó	Aviso
Bateria NVRAM descarregada (ocumEvtNvramBatteryDischarged)	Risco	Nó	Erro
Bateria NVRAM sobrecarregada (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 ela está inativa.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Status da porta inativo (ocumEvtPortStatusDown)	Incidente	Nó	Crítico

Área de impacto: desempenho

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de MB/s da porta de rede violado (ocumNetworkPortMbpsIncident)	Incidente	Porta	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite de aviso de 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 de MB/s da porta FCP violado (ocumFcpPortMbpsWarning)	Risco	Porta	Aviso
Limite crítico de utilização da porta de rede violado (ocumNetworkPortUtilizationIncident)	Incidente	Porta	Crítico
Limite de aviso de utilização de porta de rede violado (ocumNetworkPortUtilizationWarning)	Risco	Porta	Aviso
Limite crítico de utilização da porta FCP violado (ocumFcpPortUtilizationIncident)	Incidente	Porta	Crítico
Limite de aviso de utilização da porta FCP violado (ocumFcpPortUtilizationWarning)	Risco	Porta	Aviso

Eventos de fornecimento de energia

Os eventos de fontes de alimentação fornecem informações sobre o status do seu hardware para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Uma ou mais fontes de alimentação com falha (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 os problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: proteção

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Falha na tarefa de proteção (ocumEvtProtectionJobTaskFailed)	Incidente	Serviço de volume ou armazenamento	Crítico
Trabalho de proteção abortado (ocumEvtProtectionJobAborted)	Risco	Serviço de volume ou armazenamento	Aviso

Eventos Qtree

Os eventos do Qtree fornecem informações sobre a capacidade do qtree e os limites de arquivo e disco para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: capacidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Espaço Qtree quase cheio (ocumEvtQtreeSpaceNearlyFull)	Risco	Qtree	Aviso
Espaço Qtree Completo(ocumEvtQtreeSpaceFull)	Risco	Qtree	Erro

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Espaço Qtree Normal(ocumEvtQtreeSpaceThresholdOk)	Evento	Qtree	Informação
Limite máximo de arquivos Qtree atingido (ocumEvtQtreeFilesHardLimitReached)	Incidente	Qtree	Crítico
Limite suave de arquivos Qtree violado (ocumEvtQtreeFilesSoftLimitBreached)	Risco	Qtree	Aviso
Limite máximo do espaço Qtree atingido (ocumEvtQtreeSpaceHardLimitReached)	Incidente	Qtree	Crítico
Limite suave do espaço Qtree violado (ocumEvtQtreeSpaceSoftLimitBreached)	Risco	Qtree	Aviso

Eventos do processador de serviço

Os eventos do processador de serviço fornecem informações sobre o status do seu processador para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	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 seus relacionamentos assíncronos e síncronos do SnapMirror para que você possa monitorar possíveis problemas. Eventos de relacionamento SnapMirror assíncronos são gerados para VMs de armazenamento e volumes, mas eventos de relacionamento SnapMirror síncronos são gerados somente para relacionamentos de volume. Não há eventos gerados para volumes constituintes que fazem parte dos relacionamentos de recuperação de desastres da VM de armazenamento. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: proteção

Um asterisco (*) identifica eventos do EMS que foram convertidos em eventos do Unified Manager.



Os eventos de relacionamento do SnapMirror são gerados para VMs de armazenamento protegidas pela recuperação de desastres de VMs de armazenamento, mas não para quaisquer relacionamentos de objetos constituintes.

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Replicação de espelho não íntegra (ocumEvtSnapmirrorRelationshipUnhealthy)	Risco	Relacionamento SnapMirror	Aviso
Replicação de espelho interrompida (ocumEvtSnapmirrorRelationshipStateBrokenoff)	Risco	Relacionamento SnapMirror	Erro
Falha na inicialização da replicação do espelho (ocumEvtSnapmirrorRelationshipInitializeFailed)	Risco	Relacionamento SnapMirror	Erro
Falha na atualização da replicação do espelho (ocumEvtSnapmirrorRelationshipUpdateFailed)	Risco	Relacionamento SnapMirror	Erro
Erro de atraso de replicação de espelho (ocumEvtSnapMirrorRelationshipLagError)	Risco	Relacionamento SnapMirror	Erro

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Aviso de atraso de replicação de espelho (ocumEvtSnapMirrorRelationshipLagWarning)	Risco	Relacionamento SnapMirror	Aviso
Falha na ressincronização da replicação do espelho (ocumEvtSnapmirrorRelationshipResyncFailed)	Risco	Relacionamento SnapMirror	Erro
Replicação síncrona fora de sincronia *(syncSnapmirrorRelationshipOutofsync)	Risco	Relacionamento SnapMirror	Aviso
Replicação síncrona restaurada *(syncSnapmirrorRelationshipInSync)	Evento	Relacionamento SnapMirror	Informação
Falha na ressincronização automática da replicação síncrona *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Risco	Relacionamento SnapMirror	Erro
O Ontap Mediator foi adicionado ao Cluster (snapmirrorMediatorAdded)	Evento	Conjunto	Informação
O Ontap Mediator foi removido do Cluster (snapmirrorMediatorRemoved)	Evento	Conjunto	Informação
O Ontap Mediator está inacessível no cluster (snapmirrorMediatorUnreachable)	Risco	Mediador	Aviso
O Ontap Mediator não está acessível a partir do cluster (snapmirrorMediatorMisconfigured)	Risco	Mediador	Erro

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
A conectividade do Ontap Mediator foi restabelecida, ressincronizada e pronta para sincronização ativa do SnapMirror (snapmirrorMediatorInQuorum)	Evento	Mediador	Informação

Eventos de relacionamento de espelho e cofre assíncronos

Os eventos de relacionamento do SnapMirror e do Vault assíncronos fornecem informações sobre o status dos seus relacionamentos do SnapMirror e do Vault assíncronos para que você possa monitorar possíveis problemas. Eventos de relacionamento de espelho e cofre assíncronos são suportados para relacionamentos de proteção de volume e VM de armazenamento. Mas somente relacionamentos de Vault não são suportados para recuperação de desastres de VM de armazenamento. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Área de impacto: proteção



Os eventos de relacionamento SnapMirror e Vault também são gerados para VMs de armazenamento protegidas pela recuperação de desastres de VMs de armazenamento, mas não para quaisquer relacionamentos de objetos constituintes.

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Espelho e cofre assíncronos não saudáveis (ocumEvtMirrorVaultRelationshipUnhealthy)	Risco	Relacionamento SnapMirror	Aviso
Espelho e cofre assíncronos quebrados (ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risco	Relacionamento SnapMirror	Erro
Falha na inicialização do espelho e do cofre assíncronos (ocumEvtMirrorVaultRelationshipInitializeFailed)	Risco	Relacionamento SnapMirror	Erro

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Falha na atualização assíncrona do espelho e do cofre (ocumEvtMirrorVaultRelationshipUpdateFailed)	Risco	Relacionamento SnapMirror	Erro
Erro de atraso de espelho e cofre assíncrono (ocumEvtMirrorVaultRelationshipLagError)	Risco	Relacionamento SnapMirror	Erro
Aviso de atraso de espelho e cofre assíncrono (ocumEvtMirrorVaultRelationshipLagWarning)	Risco	Relacionamento SnapMirror	Aviso
Falha na ressincronização do espelho assíncrono e do cofre (ocumEvtMirrorVaultRelationshipResyncFailed)	Risco	Relacionamento SnapMirror	Erro



O evento "Falha na atualização do SnapMirror" é gerado pelo portal Active IQ (Config Advisor).

Eventos instantâneos

Os eventos de instantâneo fornecem informações sobre o status dos instantâneos, o que permite monitorar os instantâneos em busca de possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento, o nome da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Exclusão automática de instantâneo desabilitada (não aplicável)	Evento	Volume	Informação
Exclusão automática de instantâneo habilitada (não aplicável)	Evento	Volume	Informação

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Configuração de exclusão automática de instantâneo modificada (não aplicável)	Evento	Volume	Informação

Eventos de relacionamento do SnapVault

Os eventos de relacionamento do SnapVault fornecem informações sobre o status dos seus relacionamentos do SnapVault para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: proteção

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Cofre assíncrono com problemas de integridade (ocumEvtSnapVaultRelationshipUnhealthy)	Risco	Relacionamento SnapMirror	Aviso
Cofre assíncrono quebrado (ocumEvtSnapVaultRelationshipStateBrokenoff)	Risco	Relacionamento SnapMirror	Erro
Falha na inicialização do Vault assíncrono (ocumEvtSnapVaultRelationshipInitializeFailed)	Risco	Relacionamento SnapMirror	Erro
Falha na atualização do Vault assíncrono (ocumEvtSnapVaultRelationshipUpdateFailed)	Risco	Relacionamento SnapMirror	Erro
Erro de atraso do Vault assíncrono (ocumEvtSnapVaultRelationshipLagError)	Risco	Relacionamento SnapMirror	Erro
Aviso de atraso do Vault assíncrono (ocumEvtSnapVaultRelationshipLagWarning)	Risco	Relacionamento SnapMirror	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Falha na ressincronização do Vault assíncrono (ocumEvtSnapvaultRelationshipResyncFailed)	Risco	Relacionamento SnapMirror	Erro

Eventos de configurações de failover de armazenamento

Os eventos de configuração de failover de armazenamento (SFO) fornecem informações sobre se o failover de armazenamento está desabilitado ou não configurado para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Interconexão de failover de armazenamento com um ou mais links inativos (ocumEvtSfoInterconnectOneOrMoreLinksDown)	Risco	Nó	Aviso
Failover de armazenamento desabilitado (ocumEvtSfoSettingsDisabled)	Risco	Nó	Erro
Failover de armazenamento não configurado (ocumEvtSfoSettingsNotConfigured)	Risco	Nó	Erro
Estado de failover de armazenamento - aquisição (ocumEvtSfoStateTakeover)	Risco	Nó	Aviso
Estado de failover de armazenamento - Devolução parcial (ocumEvtSfoStatePartialGiveback)	Risco	Nó	Erro

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Status do nó de failover de armazenamento inativo (ocumEvtSfoNodeStatusDown)	Risco	Nó	Erro
Aquisição de failover de armazenamento não é possível (ocumEvtSfoTakeoverNotPossible)	Risco	Nó	Erro

Eventos de serviços de armazenamento

Os eventos de serviços de armazenamento fornecem informações sobre a criação e assinatura de serviços de armazenamento para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: configuração

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Serviço de armazenamento criado (não aplicável)	Evento	Serviço de armazenamento	Informação
Serviço de armazenamento assinado (não aplicável)	Evento	Serviço de armazenamento	Informação
Serviço de armazenamento cancelado (não aplicável)	Evento	Serviço de armazenamento	Informação

Área de impacto: proteção

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Exclusão inesperada do relacionamento SnapMirror gerenciadoocumEvtStorageServiceUnsupportedRelationshipDeletion	Risco	Serviço de armazenamento	Aviso
Exclusão inesperada do volume do membro do serviço de armazenamento (ocumEvtStorageServiceUnexpectedVolumeDeletion)	Incidente	Serviço de armazenamento	Crítico

Eventos de prateleiras de armazenamento

Os eventos da prateleira de armazenamento informam se sua prateleira de armazenamento está anormal para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Faixa de tensão anormal (ocumEvtShelfVoltageAbnormal)	Risco	Prateleira de armazenamento	Aviso
Faixa de corrente anormal (ocumEvtShelfCurrentAbnormal)	Risco	Prateleira de armazenamento	Aviso
Temperatura anormal (ocumEvtShelfTemperatureAbnormal)	Risco	Prateleira de armazenamento	Aviso

Eventos de VM de armazenamento

Os eventos de VM de armazenamento (máquina virtual de armazenamento, também conhecida como SVM) fornecem informações sobre o status das suas VMs de armazenamento (SVMs) para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Um asterisco (*) identifica eventos do EMS que foram convertidos em eventos do Unified Manager.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Serviço CIFS de VM de armazenamento inativo (ocumEvtVserverCifsServiceStatusDown)	Incidente	SVM	Crítico
Serviço SVM CIFS não configurado (não aplicável)	Evento	SVM	Informação
Tentativas de conectar compartilhamento CIFS inexistente *(nbladeCifsNoPrivShare)	Incidente	SVM	Crítico
Conflito de nome CIFS NetBIOS *(nbladeCifsNbNameConflict)	Risco	SVM	Erro
Falha na operação de cópia de sombra do CIFS *(cifsShadowCopyFailure)	Risco	SVM	Erro
Muitas conexões CIFS *(nbladeCifsManyAuths)	Risco	SVM	Erro
Conexão CIFS máxima excedida *(nbladeCifsMaxOpenSameFile)	Risco	SVM	Erro
Número máximo de conexões CIFS por usuário excedido *(nbladeCifsMaxSessPerUserConn)	Risco	SVM	Erro
Serviço SVM FC/FCoE inativo (ocumEvtVserverFcServiceStatusDown)	Incidente	SVM	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Serviço SVM iSCSI inativo (ocumEvtVserverIscsiServiceStatusDown)	Incidente	SVM	Crítico
Serviço NFS de VM de armazenamento inativo (ocumEvtVserverNfsServiceStatusDown)	Incidente	SVM	Crítico
Serviço SVM FC/FCoE não configurado (não aplicável)	Evento	SVM	Informação
Serviço SVM iSCSI não configurado (não aplicável)	Evento	SVM	Informação
Serviço SVM NFS não configurado (não aplicável)	Evento	SVM	Informação
VM de armazenamento interrompida (ocumEvtVserverDown)	Risco	SVM	Aviso
Servidor AV muito ocupado para aceitar nova solicitação de verificação (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

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Nenhuma conexão de servidor AV responsiva (nbladeVscanConnInactive)	Evento	SVM	Informação
Tentativa de usuário não autorizado no servidor AV (nbladeVscanBadUserPrivAccess)	Risco	SVM	Erro
Vírus encontrado pelo servidor AV (nbladeVscanVirusDetected)	Risco	SVM	Erro

Área de impacto: configuração

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
SVM descoberto (não aplicável)	Evento	SVM	Informação
SVM excluído (não aplicável)	Evento	Conjunto	Informação
SVM renomeado (não aplicável)	Evento	SVM	Informação

Área de impacto: desempenho

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de IOPS de SVM violado (ocumSvmIopsIncident)	Incidente	SVM	Crítico
Limite de aviso de IOPS SVM violado (ocumSvmIopsWarning)	Risco	SVM	Aviso
Limite crítico de SVM MB/s violado (ocumSvmMbpsIncident)	Incidente	SVM	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite de alerta de SVM MB/s violado (ocumSvmMbpsWarning)	Risco	SVM	Aviso
Limite crítico de latência de SVM violado (ocumSvmLatencyIncident)	Incidente	SVM	Crítico
Limite de aviso de latência SVM violado (ocumSvmLatencyWarning)	Risco	SVM	Aviso

Área de impacto: segurança

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Log de auditoria desabilitado (ocumVserverAuditLogDisabled)	Risco	SVM	Aviso
Banner de login desabilitado (ocumVserverLoginBannerDisabled)	Risco	SVM	Aviso
SSH está usando cifras inseguras (ocumVserverSSHInsecure)	Risco	SVM	Aviso
Banner de login alterado (ocumVserverLoginBannerChanged)	Risco	SVM	Aviso
O monitoramento anti-ransomware da VM de armazenamento está desabilitado (antiRansomwareSvmStateDisabled)	Risco	SVM	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
O monitoramento anti-ransomware da VM de armazenamento está habilitado (modo de aprendizagem) (antiRansomwareSvmStateDryrun)	Evento	SVM	Informação
VM de armazenamento adequada para monitoramento anti-ransomware (modo de aprendizagem) (ocumEvtSvmArwCandidate)	Evento	SVM	Informação

Eventos de cota de usuário 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 impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: capacidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite flexível de espaço em disco de cota de usuário ou grupo violado (ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risco	Cota de usuário ou grupo	Aviso
Limite máximo de espaço em disco de cota de usuário ou grupo atingido (ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Incidente	Cota de usuário ou grupo	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite flexível de contagem de arquivos de cota de usuário ou grupo violado (ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Risco	Cota de usuário ou grupo	Aviso
Limite máximo de contagem de arquivos de cota de usuário ou grupo atingido (ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Incidente	Cota de usuário 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 impacto e incluem o nome do evento, o nome da armadilha, o nível de impacto, o tipo de fonte e a gravidade.

Um asterisco (*) identifica eventos do EMS que foram convertidos em eventos do Unified Manager.

Área de impacto: disponibilidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Volume restrito (ocumEvtVolumeRestricted)	Risco	Volume	Aviso
Volume offline (ocumEvtVolumeOffline)	Incidente	Volume	Crítico
Volume parcialmente disponível (ocumEvtVolumePartiallyAvailable)	Risco	Volume	Erro
Volume desmontado (não aplicável)	Evento	Volume	Informação
Volume montado (não aplicável)	Evento	Volume	Informação

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Volume remontado (não aplicável)	Evento	Volume	Informação
Caminho de junção de volume inativo (ocumEvtVolumeJunctionPathInactive)	Risco	Volume	Aviso
Dimensionamento automático de volume habilitado (não aplicável)	Evento	Volume	Informação
Tamanho automático de volume desabilitado (não aplicável)	Evento	Volume	Informação
Capacidade máxima de dimensionamento automático de volume modificada (não aplicável)	Evento	Volume	Informação
Incremento de tamanho automático de volume modificado (não aplicável)	Evento	Volume	Informação

Área de impacto: capacidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Espaço de volume com provisionamento fino em risco (ocumThinProvisionVolumeSpaceAtRisk)	Risco	Volume	Aviso
Erro de operação de eficiência de volume (ocumEvtVolumeEfficiencyOperationError)	Risco	Volume	Erro
Espaço de volume completo (ocumEvtVolumeFull)	Risco	Volume	Erro

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Espaço de volume quase cheio (ocumEvtVolumeNearlyFull)	Risco	Volume	Aviso
Volume Espaço Lógico Completo (volumeLogicalSpaceFull)	Risco	Volume	Erro
Espaço lógico de volume quase cheio (volumeLogicalSpaceNearlyFull)	Risco	Volume	Aviso
Volume Espaço Lógico Normal (volumeLogicalSpaceAllOK)	Evento	Volume	Informação
Espaço de reserva de instantâneo de volume cheio (ocumEvtSnapshotFull)	Risco	Volume	Aviso
Muitas cópias de instantâneos (ocumEvtSnapshotTooMany)	Risco	Volume	Erro
Volume Qtree Quota Supercomprometido (ocumEvtVolumeQtreeQuotaOvercommitted)	Risco	Volume	Erro
Volume Qtree Quota Quase Supercomprometido (ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Risco	Volume	Aviso
Taxa de crescimento de volume anormal (ocumEvtVolumeGrowthRateAbnormal)	Risco	Volume	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Volume Dias Até Cheio (ocumEvtVolumeDaysUntilFullSoon)	Risco	Volume	Erro
Garantia de espaço de volume desabilitada (não aplicável)	Evento	Volume	Informação
Garantia de espaço de volume habilitada (não aplicável)	Evento	Volume	Informação
Garantia de espaço de volume modificada (não aplicável)	Evento	Volume	Informação
Dias de reserva do instantâneo de volume até o limite máximo (ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risco	Volume	Erro
Os constituintes do FlexGroup têm problemas de espaço *(flexGroupConstituentsHaveSpaceIssues)	Risco	Volume	Erro
Status do espaço dos constituintes do FlexGroup : Tudo OK *(flexGroupConstituentsSpaceStatusAllOK)	Evento	Volume	Informação
Os constituintes do FlexGroup têm problemas com inodes *(flexGroupConstituentsHaveNodesIssues)	Risco	Volume	Erro
Status dos inodes dos constituintes do FlexGroup Todos OK *(flexGroupConstituentsInodesStatusAllOK)	Evento	Volume	Informação

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Falha no dimensionamento automático do volume WAFL *(wafIVolAutoSizeFail)	Risco	Volume	Erro
WAFL Volume AutoSize Concluído *(wafIVolAutoSizeDone)	Evento	Volume	Informação
O volume do FlexGroup é utilizado em mais de 80%*	Incidente	Volume	Erro
O volume do FlexGroup é utilizado em mais de 90%*	Incidente	Volume	Crítico
Anomalia de eficiência de armazenamento de volume (ocumVolumeAbnormalStorageEfficiencyWarning)	Risco	Volume	Aviso
Reserva de instantâneo de volume subutilizada (volumeSnapshotReserveUnderutilizedWarning)	Evento	Volume	Aviso
Reserva de instantâneo de volume subutilizada (volumeSnapshotReserveUnderutilizedCleared)	Evento	Volume	Aviso

Área de impacto: configuração

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Volume renomeado (não aplicável)	Evento	Volume	Informação
Volume descoberto (não aplicável)	Evento	Volume	Informação

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Volume excluído (não aplicável)	Evento	Volume	Informação

Área de impacto: desempenho

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite de aviso de IOPS máximo de volume de QoS violado (ocumQosVolumeMaxlopsWarning)	Risco	Volume	Aviso
Limite de alerta de volume máximo de MB/s de QoS violado (ocumQosVolumeMaxMbpsWarning)	Risco	Volume	Aviso
Limite de alerta de IOPS/TB de volume máximo de QoS violado (ocumQosVolumeMaxlopsPerTbWarning)	Risco	Volume	Aviso
Limite de latência do 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

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de volume MB/s violado (ocumVolumeMbpsIncident)	Incidente	Volume	Crítico
Limite de alerta de volume MB/s 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
Limite crítico de taxa de falha de cache de volume violado (ocumVolumeCacheMissRatioIncident)	Incidente	Volume	Crítico
Limite de aviso de taxa de falha de cache de volume violado (ocumVolumeCacheMissRatioWarning)	Risco	Volume	Aviso
Limite crítico de latência de volume e IOPS violado (ocumVolumeLatencyIopsIncident)	Incidente	Volume	Crítico
Limite de alerta de latência de volume e IOPS violado (ocumVolumeLatencyIopsWarning)	Risco	Volume	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Latência de volume e limite crítico de MB/s violado (ocumVolumeLatencyMbpsIncident)	Incidente	Volume	Crítico
Limite de alerta de latência de volume e MB/s violado (ocumVolumeLatencyMbpsWarning)	Risco	Volume	Aviso
Limite crítico de latência de volume e capacidade de desempenho agregado violado (ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Incidente	Volume	Crítico
Limite de aviso de latência de volume e capacidade de desempenho agregado usada violado (ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Risco	Volume	Aviso
Limite crítico de latência de volume e utilização agregada violado (ocumVolumeLatencyAggregateUtilizationIncident)	Incidente	Volume	Crítico
Limite de aviso de latência de volume e utilização agregada violado (ocumVolumeLatencyAggregateUtilizationWarning)	Risco	Volume	Aviso

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Limite crítico de latência de volume e capacidade de desempenho do nó violado (ocumVolumeLatencyNodePerfCapacityUsedIncident)	Incidente	Volume	Crítico
Limite de aviso de capacidade usada de desempenho de nó e latência de volume 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
Limite crítico de latência de volume 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 impacto: segurança

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
O monitoramento anti-ransomware de volume está habilitado (modo ativo) (antiRansomwareVolumeStateEnabled)	Evento	Volume	Informação
O monitoramento anti-ransomware de volume está desabilitado (antiRansomwareVolumeStateDisabled)	Risco	Volume	Aviso
O monitoramento anti-ransomware de volume está habilitado (modo de aprendizagem) (antiRansomwareVolumeStateDryrun)	Evento	Volume	Informação
O monitoramento anti-ransomware de volume está pausado (modo de aprendizagem) (antiRansomwareVolumeStateDryrunPaused)	Risco	Volume	Aviso
O monitoramento anti-ransomware de volume está pausado (modo ativo) (antiRansomwareVolumeStateEnablePaused)	Risco	Volume	Aviso
O monitoramento anti-ransomware de volume está desabilitado (antiRansomwareVolumeStateDisableInProgress)	Risco	Volume	Aviso
Atividade de ransomware observada (callHomeRansomwareActivitySeen)	Incidente	Volume	Crítico

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Volume adequado para monitoramento anti-ransomware (modo de aprendizagem) (ocumEvtVolumeArwCandidate)	Evento	Volume	Informação
Volume adequado para monitoramento anti-ransomware (modo ativo) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Risco	Volume	Aviso
O volume exibe alertas anti-ransomware ruidosos (antiRansomwareFeatureNoisyVolume)	Risco	Volume	Aviso

Área de impacto: proteção de dados

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
O volume tem proteção de instantâneo local insuficiente (volumeLacksLocalProtectionWarning)	Risco	Volume	Aviso
O volume tem proteção de instantâneo local insuficiente (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 do seu volume para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da armadilha, nível de impacto, tipo de fonte e gravidade.

Área de impacto: capacidade

Nome do evento (nome da armadilha)	Nível de impacto	Tipo de fonte	Gravidade
Status da movimentação de volume: Em andamento (não aplicável)	Evento	Volume	Informação
Status de movimentação de volume - Falha (ocumEvtVolumeMoveFailed)	Risco	Volume	Erro
Status da movimentação de volume: Concluído (não aplicável)	Evento	Volume	Informação
Movimento de volume - Corte adiado (ocumEvtVolumeMoveCutoverDeferred)	Risco	Volume	Aviso

Descrição das janelas de eventos e caixas de diálogo

Os eventos notificam você sobre quaisquer problemas no 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. Você pode usar a página Configuração de eventos para desabilitar ou habilitar eventos.

Página de notificações

Você pode configurar o servidor do Unified Manager para enviar notificações quando um evento for gerado ou quando for atribuído a um usuário. Você também pode configurar os mecanismos de notificação. Por exemplo, notificações podem ser enviadas como e-mails ou traps SNMP.

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

E-mail

Esta área permite que você configure as seguintes configurações de e-mail para notificação de alerta:

- **Endereço de origem**

Especifica o endereço de e-mail do qual a notificação de alerta é enviada. Este valor também é usado como endereço de origem para um relatório quando compartilhado. Se o Endereço De estiver preenchido com o endereço "ActiveIQUnifiedManager@localhost.com", você deverá alterá-lo para um endereço de e-mail real e funcional para garantir que todas as notificações por e-mail sejam entregues com sucesso.

Servidor SMTP

Esta área permite que você configure as seguintes configurações do servidor SMTP:

- **Nome do host ou endereço IP**

Especifica o nome do host do seu servidor host SMTP, que é usado para enviar a notificação de alerta aos destinatários especificados.

- **Nome de usuário**

Especifica o nome de usuário SMTP. O nome de usuário SMTP é necessário somente quando o SMTPAUTH está habilitado no servidor SMTP.

- **Senha**

Especifica a senha SMTP. O nome de usuário SMTP é necessário somente quando o SMTPAUTH está habilitado no servidor SMTP.

- **Porta**

Especifica a porta usada pelo servidor host SMTP para enviar notificações 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 que você configure as seguintes configurações de interceptação SNMP:

- **Versão**

Especifica a versão SNMP que você deseja usar dependendo do tipo de segurança necessária. As opções incluem Versão 1, Versão 3, Versão 3 com Autenticação e Versão 3 com Autenticação e Criptografia. O valor padrão é Versão 1.

- **Anfitrião do Destino da Armadilha**

Especifica o nome do host ou endereço IP (IPv4 ou IPv6) que recebe as interceptações SNMP enviadas pelo servidor de gerenciamento. Para especificar vários destinos de interceptação, 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 na lista.

- **Porta de Armadilha de Saída**

Especifica a porta pela qual o servidor SNMP recebe as interceptações enviadas pelo servidor de gerenciamento.

O valor padrão é 162.

- **Comunidade**

A sequência de caracteres da comunidade para acessar o host.

- **ID do motor**

Especifica o identificador exclusivo do agente SNMP e é gerado automaticamente pelo servidor de gerenciamento. O Engine ID está disponível com SNMP Versão 3, SNMP Versão 3 com Autenticação e SNMP Versão 3 com Autenticação e Criptografia.

- **Nome de usuário**

Especifica o nome de usuário SNMP. O nome de usuário está disponível com SNMP versão 3, SNMP versão 3 com autenticação e SNMP versão 3 com autenticação e criptografia.

- **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 Criptografia.

- **Senha de autenticação**

Especifica a senha usada ao autenticar um usuário. A senha de autenticação está disponível com SNMP Versão 3 com Autenticação e SNMP Versão 3 com Autenticação e Criptografia.

- **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 SNMP Versão 3 com Autenticação e Criptografia.

- **Senha de privacidade**

Especifica a senha ao usar o protocolo de privacidade. A senha de privacidade está disponível com SNMP versão 3 com autenticação e criptografia.

Para obter mais informações sobre objetos e armadilhas SNMP, você pode baixar o "[MIB do Active IQ Unified Manager](#)" do site de suporte da NetApp .

Página de inventário de gerenciamento de eventos

A página de inventário do Gerenciamento de Eventos permite que você visualize 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 eventos mais recentes sejam exibidos.

Componentes do filtro

Permite que você personalize as informações exibidas na lista de eventos. Você pode refinar a lista de eventos exibidos usando os seguintes componentes:

- Menu Exibir para selecionar em uma lista predefinida de seleções de filtros.

Isso inclui itens como todos os eventos ativos (novos e reconhecidos), eventos de desempenho ativos, 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 todos os campos e atributos de campo disponíveis para refinar a lista de eventos.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Atribuir a**

Permite que você selecione o usuário ao qual o evento será atribuído. Quando você atribui um evento a um usuário, o nome do usuário e a hora em que você atribuiu o evento são adicionados à lista de eventos dos eventos selecionados.

- Meu

Atribui o evento ao usuário conectado no momento.

- Outro usuário

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 de propriedade em branco.

- **Reconhecer**

Reconhece os eventos selecionados.

Quando você reconhece um evento, seu nome de usuário e o horário em que você reconheceu o evento são adicionados à lista de eventos selecionados. Quando você reconhece um evento, você é responsável por gerenciá-lo.



Você não pode reconhecer eventos de informação.

- **Marcar como resolvido**

Permite que você altere o estado do evento para resolvido.

Quando você resolve um evento, seu nome de usuário e o horário em que você resolveu o evento são adicionados à lista de eventos selecionados. Depois de tomar a ação corretiva para o evento, você deve marcá-lo como resolvido.

- **Adicionar alerta**

Exibe a caixa de diálogo Adicionar alerta, que permite adicionar alertas para os eventos selecionados.

- **Relatórios**

Permite exportar detalhes da visualização do evento atual para um arquivo de valores separados por vírgulas (.csv) ou documento PDF.

- **Mostrar/Ocultar Seletor de Colunas**

Permite que você escolha as colunas que serão exibidas na página e selecione a ordem em que elas serão exibidas.

Lista de eventos

Exibe detalhes de todos os eventos ordenados por tempo de disparo.

Por padrão, a visualização Todos os eventos ativos é exibida para mostrar os eventos novos e confirmados dos últimos sete dias que têm um Nível de Impacto de Incidente ou Risco.

- **Tempo Acionado**

A hora em que o evento foi gerado.

- **Gravidade**

Gravidade do evento: Crítico (❌), Erro (⚠️), Aviso (⚠️) e Informações (ℹ️).

- **Estado**

O estado do evento: Novo, Reconhecido, Resolvido ou Obsoleto.

- **Nível de Impacto**

O nível de impacto do evento: Incidente, Risco, Evento ou Atualização.

- **Área de Impacto**

Área de impacto do evento: Disponibilidade, Capacidade, Desempenho, Proteção, Configuração ou Segurança.

- **Nome**

O nome do evento. Você pode selecionar o nome para exibir a página 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 desse objeto.

Quando ocorre uma violação da política de QoS compartilhada, somente o objeto de carga de trabalho que está consumindo mais IOPS ou MB/s é mostrado neste campo. Cargas de trabalho adicionais que usam esta política são exibidas na página Detalhes do evento.

- **Tipo de fonte**

O tipo de objeto (por exemplo, VM de armazenamento, volume ou Qtree) ao 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 "Active IQ Portal" ou diretamente no "Active IQ Unified Manager".

- **Nome da anotação**

O nome da anotação atribuída ao objeto de armazenamento.

- **Notas**

O número de notas adicionadas para um evento.

- **Dias pendentes**

O número de dias desde que o evento foi gerado inicialmente.

- **Tempo Atribuído**

O tempo decorrido desde que o evento foi atribuído a um usuário. Se o tempo decorrido exceder uma semana, o registro de data e hora em que o evento foi atribuído a um usuário será exibido.

- **Reconhecido por**

O nome do usuário que reconheceu o evento. O campo ficará 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, o registro de data e hora em que o evento foi reconhecido será exibido.

- **Resolvido por**

O nome do usuário que resolveu o evento. O campo ficará 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 registro de data e hora em que o evento foi resolvido será exibido.

- **Tempo Obsoleto**

O momento em que o estado do evento se tornou obsoleto.

Página de detalhes do evento

Na página Detalhes do evento, você pode visualizar os detalhes de um evento selecionado, como gravidade do evento, nível de impacto, área de impacto e origem do evento. Você também pode visualizar informações adicionais sobre possíveis soluções 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 sem desempenho, enquanto o evento estiver no estado Novo ou Reconhecido, as últimas informações vistas não serão conhecidas e, portanto, ficarão ocultas.

- **Descrição do Evento**

Uma breve descrição do evento.

Em alguns casos, o motivo do 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 em disputa, seu ícone será circulado e destacado em vermelho.

Consulte *Componentes do cluster e por que eles podem estar em disputa* para obter uma descrição dos componentes exibidos aqui.

As seções Informações do evento, Diagnóstico do sistema e Ações sugeridas são descritas em outros tópicos.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Ícone de notas**

Permite que você adicione ou atualize uma nota sobre o evento e revise todas as notas deixadas por outros usuários.

Menu de 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 à lista de eventos dos eventos selecionados.

Você também pode cancelar a atribuição de eventos deixando o campo de propriedade em branco.

- **Reconhecer**

Reconhece os eventos selecionados para que você não continue recebendo notificações de alerta repetidas.

Quando você reconhece um evento, seu nome de usuário e o horário em que você reconheceu o evento são adicionados à lista de eventos (Reconhecido por) para os eventos selecionados. Quando você

reconhece um evento, você assume a responsabilidade de gerenciá-lo.

- **Marcar como resolvido**

Permite que você altere o estado do evento para Resolvido.

Quando você resolve um evento, seu nome de usuário e o horário em que você resolveu o evento são adicionados à lista de eventos (Resolvido por) para os eventos selecionados. Depois de tomar a ação corretiva para o evento, você deve marcá-lo 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

Use a seção Informações do evento na página Detalhes do evento para visualizar os detalhes sobre um evento selecionado, como gravidade do evento, nível de impacto, área de impacto e origem do evento.

Os campos que não são aplicáveis ao tipo de evento são ocultados. Você pode visualizar os seguintes detalhes do evento:

- **Hora do acionamento do evento**

A hora 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 se tornasse 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, esse é o tempo entre a detecção e a resolução do evento.

Este campo é exibido para todos os eventos de desempenho e para outros tipos de eventos somente depois que eles forem resolvidos ou se tornarem obsoletos.

- **Visto pela última vez**

A data e a hora em que o evento foi visto pela última vez como ativo.

Para eventos de desempenho, esse valor pode ser mais recente que o Tempo de acionamento do evento, pois esse campo é atualizado após cada nova coleta de dados de desempenho, desde que o evento esteja ativo. Para outros tipos de eventos, quando no estado Novo ou Reconhecido, esse conteúdo não é atualizado e, portanto, o campo fica oculto.

- **Gravidade**

Gravidade do evento: Crítico (❌), Erro (💡), Aviso (⚠️) e Informações (ℹ️).

- **Nível de Impacto**

O nível de impacto do evento: Incidente, Risco, Evento ou Atualização.

- **Área de Impacto**

Área de impacto do evento: Disponibilidade, Capacidade, Desempenho, Proteção, Configuração ou Segurança.

- **Fonte**

O nome do objeto no qual o evento ocorreu.

Ao visualizar os detalhes de um evento de política de QoS compartilhada, até três dos objetos de carga de trabalho que estão consumindo mais 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 da fonte**

Exibe o nome e o valor da anotação para o objeto ao qual o evento está associado.

Este campo é exibido somente 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.

Este campo é exibido somente 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 do objeto para exibir a página de inventário preenchida com os objetos que estão atualmente afetados por este evento.

Este campo é exibido somente para eventos de performance.

- **Volumes afetados**

O número de volumes que estão sendo afetados por este evento.

Este campo é exibido somente 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 somente para eventos de performance.

- **ID da regra**

Para eventos da plataforma Active IQ , este 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 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.

Alertas desabilitados não são exibidos.

- **Última notificação enviada**

Data e hora em que a notificação de alerta mais recente foi enviada.

- **Enviar por**

O mecanismo usado para enviar a notificação de alerta: e-mail ou trap SNMP.

- **Execução de script anterior**

O nome do script que foi executado quando o alerta foi gerado.

O que a seção **Ações sugeridas** exibe

A seção **Ações sugeridas** da página **Detalhes do evento** fornece possíveis motivos para o evento e sugere algumas ações para que você possa tentar resolver o evento sozinho. As ações sugeridas são personalizadas com base no tipo de evento ou tipo de limite que foi violado.

Esta área é exibida apenas para alguns tipos de eventos.

Em alguns casos, há links de **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 do Unified Manager, do ONTAP System Manager, do OnCommand Workflow Automation, dos comandos ONTAP CLI ou de uma combinação dessas ferramentas.

Você deve considerar as ações sugeridas aqui apenas como um guia para resolver este evento. A ação que você tomar para resolver esse evento deve ser baseada no contexto do seu ambiente.

Se você quiser analisar o objeto e o evento com mais detalhes, clique no botão **Analisar carga de trabalho** para exibir a página **Análise de carga de trabalho**.

Há certos eventos que o Unified Manager pode diagnosticar completamente e fornecer uma única resolução. Quando disponíveis, essas resoluções são exibidas com um botão **Corrigir**. Clique neste botão para que o Unified Manager corrija o problema que está causando o evento.

Para eventos da plataforma Active IQ, esta seção pode conter um link para um artigo da Base de conhecimento da NetApp, quando disponível, que descreve o problema e as possíveis soluções. 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 a seção **Diagnóstico do Sistema** exibe

A seção **Diagnóstico do Sistema** da página **Detalhes do Evento** fornece informações que podem ajudar você a diagnosticar problemas que podem ter sido responsáveis pelo evento.

Esta área é exibida apenas para alguns eventos.

Alguns eventos de desempenho fornecem gráficos relevantes para o evento específico que foi acionado. Normalmente, isso inclui um gráfico de IOPS ou MBps e um gráfico de latência dos dez dias anteriores. Quando organizados dessa forma, você pode ver quais componentes de armazenamento estão mais 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 da carga de trabalho** - Exibe detalhes sobre o uso da carga de trabalho do componente do cluster em contenção.
- **Atividade de recurso** - Exibe estatísticas históricas de desempenho para o componente do cluster em contenção.

Outros gráficos são exibidos quando alguns componentes do cluster estão em disputa.

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 que foi analisado, para políticas de desempenho definidas pelo sistema que analisam vários contadores de desempenho. Nesse cenário, um ícone verde ou vermelho é exibido ao lado do diagnóstico para indicar se um problema foi encontrado ou não naquele diagnóstico específico.

Página de configuração do evento

A página Configuração de evento exibe a lista de eventos que estão desabilitados 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 poderá acessar esta página se tiver a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas para eventos selecionados:

- **Desativar**

Inicia a caixa de diálogo Desativar eventos, que você pode usar para desativar eventos.

- **Habilitar**

Habilita eventos selecionados que você escolheu desabilitar anteriormente.

- **Regras de upload**

Inicia a caixa de diálogo Regras de upload, que permite que sites sem acesso à rede externa carreguem manualmente o arquivo de regras do Active IQ para o Unified Manager. As regras são executadas em mensagens do AutoSupport do cluster para gerar eventos para configuração do sistema, cabeamento, práticas recomendadas e disponibilidade, conforme definido pela plataforma Active IQ .

- **Inscriva-se nos eventos do EMS**

Inicia a caixa de diálogo Inscrever-se em eventos do 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 coleta informações sobre eventos que ocorrem no cluster. Quando uma notificação é recebida para um evento EMS inscrito, um evento do Unified Manager é gerado com a gravidade apropriada.

Visualização de lista

A exibição de lista exibe (em formato tabular) informações sobre eventos que estão desabilitados. Você pode usar os filtros de coluna para personalizar os dados exibidos.

- **Evento**

Exibe o nome do evento que está desabilitado.

- **Gravidade**

Exibe a gravidade do evento. A gravidade pode ser Crítica, Erro, Aviso ou Informação.

- **Tipo de fonte**

Exibe o tipo de fonte para a qual o evento é gerado.

Caixa de diálogo Desativar eventos

A caixa de diálogo Desabilitar eventos exibe a lista de tipos de eventos para os quais você pode desabilitar eventos. Você pode desabilitar eventos para um tipo de evento com base em uma gravidade específica ou para um conjunto de eventos.

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Área de 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 Crítico, Erro, Aviso ou Informação.

- **Nome do evento contém**

Permite filtrar eventos cujo nome contém os caracteres especificados.

- **Eventos correspondentes**

Exibe a lista de eventos correspondentes ao tipo de gravidade do evento e à sequência de texto especificada.

- **Desativar eventos**

Exibe a lista de eventos que você selecionou para desabilitar.

A gravidade do evento também é exibida junto com o nome do evento.

Botões de comando

Os botões de comando permitem que você execute 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.

Gerenciar alertas

Você pode configurar alertas para enviar notificações automaticamente quando ocorrerem eventos específicos ou eventos de certos tipos de gravidade. Você também pode associar um alerta a um script que é executado quando um alerta é disparado.

O que são 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 disparado.

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 que foi violado para causar o evento e uma descrição do evento. A mensagem de e-mail também fornece um hiperlink para cada evento que permite que você visualize a página de detalhes do evento na interface do usuário.

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 poderá fazer com que um evento crítico e um evento de aviso sejam acionados ao mesmo tempo para a mesma política de limite. Nesse caso, você pode receber um e-mail para o evento de aviso e outro para o evento crítico. Isso ocorre porque o Unified Manager permite que você assine separadamente para receber alertas de avisos 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 for 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 as configurações de notificação, como o endereço de e-mail do usuário, o servidor SMTP e o host de interceptação SNMP para permitir que o servidor Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento for gerado.
- Você deve saber os recursos e eventos para os quais deseja acionar o alerta, além dos nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se quiser que um script seja executado com base no evento, você deve adicionar o script ao Unified Manager usando a página Scripts.
- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode criar um alerta diretamente na página Detalhes do evento após 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 sequência de texto no campo **Nome contém** para selecionar um grupo de recursos. Com base na sequência de texto especificada, a lista de recursos disponíveis exibe apenas aqueles que correspondem à regra de filtro. A sequência de texto que você especificar diferencia maiúsculas de minúsculas.

Se um recurso estiver em conformidade com as regras de inclusão e exclusão especificadas, a regra de exclusão terá precedência sobre a regra de inclusão, 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 o qual você deseja acionar um alerta.



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

6. Clique em **Ações** e selecione os usuários que deseja notificar, escolha a frequência de notificação, escolha se uma armadilha SNMP será enviada ao receptor da armadilha 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 aparecerá em branco porque o endereço de e-mail modificado não estará mais mapeado para o usuário selecionado anteriormente. Além disso, se você modificar 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 por meio de traps SNMP.

7. Clique em **Salvar**.

Exemplo de adição de um alerta

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

- Nome do alerta: HealthTest
- Recursos: inclui todos os volumes cujo nome contém "abc" e exclui todos os volumes cujo nome contém "xyz"
- Eventos: inclui todos os eventos críticos de saúde
- Ações: inclui "sample@domain.com", um script de "Teste" e o usuário deve ser notificado a cada 15 minutos

Execute as seguintes etapas na caixa de diálogo Adicionar alerta:

1. Clique em **Nome** e digite *HealthTest * no campo **Nome do alerta**.
2. Clique em **Recursos** e, na guia Incluir, selecione **Volumes** na lista suspensa.
 - a. Digitar *abc * no campo **Nome contém** para exibir os volumes cujo nome contém "abc".
 - b. Selecione **+ [All Volumes whose name contains 'abc'] +** da 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 **Crítico** no campo Gravidade do Evento.
 4. Selecione **Todos os Eventos Críticos** na área Eventos Correspondentes e mova-os para a área Eventos Seleccionados.
 5. Clique em **Ações** e digite *sample@domain.com * no campo Alertar estes usuários.
 6. Selecione **Lembrar a cada 15 minutos** para notificar o usuário a cada 15 minutos.
- Você pode configurar um alerta para enviar notificações repetidamente aos destinatários por um período específico. Você deve determinar o horário a partir do qual a notificação de evento estará ativa para o alerta.
7. No menu Selecionar script para executar, selecione o script **Teste**.
 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 ajude você a rastreá-los 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, deverá selecionar 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.



Selecionar 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 de todos os clusters, receberá alertas somente para eventos críticos do cluster. Você não receberá alertas para 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, deverá decidir quais eventos exigem um

alerta.

Se você selecionar uma gravidade de evento, mas não selecionar nenhum evento individual (se deixar a coluna "Eventos selecionados" vazia), você receberá alertas para todos os eventos na categoria.

- **Ações**

Você deve fornecer os nomes de usuário e endereços de e-mail dos usuários que receberão a notificação. Você também pode especificar uma interceptação SNMP como modo de notificação. Você pode associar seus scripts a um alerta para que eles sejam executados quando um alerta for gerado.

- **Frequência de notificação**

Você pode configurar um alerta para enviar notificações repetidamente aos destinatários por um período específico. Você deve determinar o horário a partir do qual a notificação de evento estará ativa para o alerta. Se quiser que a notificação do evento seja repetida até que o evento seja reconhecido, você deve determinar com que frequência deseja que a notificação seja repetida.

- **Executar script**

Você pode associar seu script a um alerta. Seu script é executado quando o alerta é gerado.

Adicionar alertas para eventos de desempenho

Você pode configurar alertas para eventos de desempenho individuais, assim como quaisquer outros eventos recebidos pelo Unified Manager. Além disso, se você quiser tratar todos os eventos de desempenho da mesma forma e enviar e-mails para a mesma pessoa, você pode criar um único alerta para notificá-lo quando qualquer evento de desempenho crítico ou de aviso for acionado.

Antes de começar

Você deve ter a função de Administrador de Aplicativos 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 nenhum recurso é selecionado, 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 Severidade do Evento, selecione **Crítico**.
 - b. No campo Nome do evento contém, insira `*latency*` e então clique na seta para selecionar todos os eventos correspondentes.

- c. No campo Nome do evento contém, insira *iops * e então clique na seta para selecionar todos os eventos correspondentes.
- d. No campo Nome do evento contém, insira *mbps * e então 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 estes usuários**.
7. Configure quaisquer outras opções nesta página para emitir traps SNMP e executar um script.
8. Clique em **Salvar**.

Alertas de teste

Você pode testar um alerta para verificar se ele foi configurado 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 foi enviada e se o seu script foi executado usando o alerta de teste.

Antes de começar

- Você deve ter configurado as configurações de notificação, como o endereço de e-mail dos destinatários, o servidor SMTP e a interceptação 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 for gerado.
- Você deve ter a função de Administrador do Aplicativo.

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 **Testar**.

Um e-mail de alerta de teste é enviado para os endereços de e-mail que você especificou ao criar o alerta.

Habilitar e desabilitar 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, Reconhecido, Resolvido e Obsoleto. Se não quiser receber alertas sobre eventos conforme eles passam para os estados Resolvido e Obsoleto, você pode configurar uma configuração global para suprimir esses alertas.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Por padrão, os alertas não são enviados para eventos à medida que eles passam 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 quando os eventos forem resolvidos ou se tornarem obsoletos	Mova o controle deslizante para a esquerda
Comece a enviar alertas conforme os eventos forem resolvidos ou se tornarem obsoletos	Mova o controle deslizante para a direita

Excluir volumes de destino de recuperação de desastres da geração de alertas

Ao configurar alertas de volume, você pode especificar uma sequência de caracteres na caixa de diálogo Alerta que identifica um volume ou grupo de volumes. No entanto, se você tiver configurado a recuperação de desastres para SVMs, os volumes de origem e destino terão o mesmo nome, então você receberá alertas para ambos os volumes.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode desabilitar alertas para 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 "<nome_svm>:/<nome_volume>".

O exemplo abaixo mostra como criar alertas para o volume "vol1" no SVM primário "vs1", mas excluir o alerta de ser 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 aba **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'] +** da área **Recursos Disponíveis** e mova-o para a área **Recursos Selecionados**.
3. Selecione a aba **Excluir**, selecione **Volume**, digite *vs1-dr * no campo **Nome contém** e clique em **Adicionar**.

Isso exclui a geração do alerta para o volume "vol1" no SVM "vs1-dr".

4. Clique em **Eventos** e selecione o evento ou eventos que você 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 estes usuários**.
6. Configure quaisquer outras opções nesta página para emitir traps SNMP e executar um script e, em

seguida, clique em **Salvar**.

Ver alertas

Você pode visualizar a lista de alertas criada para vários eventos na página Configuração de alertas. Você também pode visualizar 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

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Etapas

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 ao qual o alerta está associado, eventos, destinatários, opções de notificação, frequência de notificação e scripts associados.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

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 de nome, recursos, eventos e ações, conforme necessário.

Você pode alterar ou remover o script associado ao alerta.

4. Clique em **Salvar**.

Excluir 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

Você deve ter a função de Administrador do Aplicativo.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de alerta**.
2. Na página **Configuração de alertas**, selecione os alertas que deseja excluir e clique em **Excluir**.
3. Clique em **Sim** 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. Você também pode visualizar a lista de alertas na página Configuração de alertas.

Página de configuração de alerta

A página Configuração de alerta exibe uma lista de alertas e fornece informações sobre o nome do alerta, status, método de notificação e frequência de notificação. Você também pode adicionar, editar, remover, habilitar ou desabilitar alertas nesta página.

Você deve ter a função de Administrador de Aplicativos 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**

Exclui os alertas selecionados.

- **Habilitar**

Habilita 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 após serem adicionados ou editados.

- **Alertas para eventos resolvidos e obsoletos**

Permite habilitar ou desabilitar o envio de alertas quando eventos são movidos para os estados Resolvido ou Obsoleto. Isso pode ajudar os usuários a não receberem notificações desnecessárias.

Visualização 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 ver mais informações sobre ele na área de detalhes.

- **Status**

Especifica se um alerta está habilitado () ou desabilitado () .

- **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 por e-mail ou traps SNMP.

- **Frequência de Notificação**

Especifica a frequência (em minutos) com que o servidor de gerenciamento continua enviando 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 do alerta.

- **Frequência de Notificação**

Exibe a frequência com que o servidor de gerenciamento continua enviando 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 do 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 for gerado, para que você possa resolver o problema rapidamente e, assim, minimizar o impacto 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.

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Nome

Esta área permite que você especifique um nome e uma descrição para o alerta:

- **Nome do Alerta**

Permite que você especifique um nome de alerta.

- **Descrição do Alerta**

Permite que você especifique uma descrição para o alerta.

Recursos

Esta área permite que você selecione um recurso individual ou agrupe 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 sequência de texto que você especifica. Você pode pesquisar recursos selecionando um tipo de recurso na lista suspensa ou pode especificar o nome exato do recurso para exibir um recurso específico.

Se você estiver criando um alerta de qualquer uma das páginas de detalhes do objeto de armazenamento, o objeto de armazenamento será automaticamente incluído no alerta.

- **Incluir**

Permite que você inclua os recursos para os quais deseja acionar alertas. Você pode especificar uma

sequência de texto para agrupar recursos que correspondem à sequência e selecionar esse grupo para ser incluído no alerta. Por exemplo, você pode agrupar todos os volumes cujo nome contém a string "abc".

- **Excluir**

Permite que você exclua recursos para os quais 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, [+\[All Volumes\]](#) ou [\[All Volumes whose name contains 'xyz'\]](#) +.

Se um recurso estiver em conformidade com as regras de inclusão e exclusão especificadas, a regra de exclusão terá precedência sobre a regra de inclusão e o alerta não será gerado para o evento.

Eventos

Esta área permite que você selecione os eventos para os quais deseja criar os alertas. Você pode criar alertas para eventos com base em uma gravidade específica ou para um conjunto de eventos.

Para selecionar mais de um evento, você deve manter pressionada a tecla Ctrl enquanto faz suas 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

Esta área permite que você especifique os usuários que deseja notificar quando um alerta for disparado. Você também pode especificar o método de notificação e a frequência da notificação.

- **Alertar esses usuários**

Permite que você especifique o endereço de e-mail ou nome de usuário do usuário que receberá notificações.

Se você modificar o endereço de e-mail especificado para o usuário e reabrir o alerta para edição, o campo Nome aparecerá em branco porque o endereço de e-mail modificado não estará 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 que você especifique 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 com uma frequência específica

- Notificar em uma frequência específica dentro do intervalo de tempo especificado

- **Emitir armadilha SNMP**

Selecionar esta caixa permite que você especifique se as intercepções SNMP devem ser enviadas ao host SNMP configurado globalmente.

- **Executar Script**

Permite que você adicione 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 desabilitada pelo seu administrador. Se necessário, você pode habilitar essa funcionalidade em **Gerenciamento de armazenamento > Configurações de recursos**.

Botões de comando

- **Salvar**

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 ao qual o alerta está associado, eventos, script e opções de notificação.

Nome

Esta área permite que você edite o nome e a descrição do alerta.

- **Nome do Alerta**

Permite que você edite o nome do alerta.

- **Descrição do Alerta**

Permite que você especifique uma descrição para o alerta.

- **Estado de Alerta**

Permite que você habilite ou desabilite o alerta.

Recursos

Esta área permite que você selecione um recurso individual ou agrupe 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 pode especificar o nome exato do recurso para exibir um recurso específico.

- **Incluir**

Permite que você inclua os recursos para os quais deseja acionar alertas. Você pode especificar uma sequência de texto para agrupar recursos que correspondem à sequência e selecionar esse grupo para ser incluído no alerta. Por exemplo, você pode agrupar todos os volumes cujo nome contém a string “vol0”.

- **Excluir**

Permite que você exclua recursos para os quais 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] + ou +[All Volumes whose name contains 'xyz'] +.

Eventos

Esta área permite que você selecione os eventos para os quais deseja acionar os alertas. Você pode acionar um alerta para eventos com base em uma gravidade específica ou para 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 que você especifique o método de notificação e a frequência da notificação.

- **Alertar esses usuários**

Permite que você edite o endereço de e-mail ou nome de usuário, ou especifique um novo endereço de e-mail ou nome de usuário para receber notificações.

- **Frequência de Notificação**

Permite que você edite 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 com uma frequência específica
- Notificar em uma frequência específica dentro do intervalo de tempo especificado

- **Emitir armadilha SNMP**

Permite que você especifique se as interceptações SNMP devem ser enviadas ao host SNMP configurado globalmente.

- **Executar Script**

Permite que você associe um script ao alerta. Este script é executado quando um alerta é gerado.

Botões de comando

- **Salvar**

Salva as alterações e fecha a caixa de diálogo.

- **Cancelar**

Descarta as alterações e fecha a caixa de diálogo.

Gerenciar 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 dispara um alerta, o script é executado. Você pode carregar scripts personalizados e testar sua execução quando um alerta for gerado.

A capacidade de carregar scripts no Unified Manager e executá-los é habilitada por padrão. Se sua organização não quiser permitir essa funcionalidade por motivos de segurança, você pode desabilitá-la em **Gerenciamento de armazenamento > Configurações de recursos**.

Informações relacionadas

["Habilitando e desabilitando a capacidade de fazer upload de scripts"](#)

Como os scripts funcionam com alertas

Você pode associar um alerta ao seu script para que ele 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 tiver associado um alerta a um script, o script será executado. Você pode obter os detalhes dos argumentos passados ao script no 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 executadas com base no seu script personalizado para esse tipo de evento, e as ações **Corrigir** 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 reunir 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`
```

Adicionar scripts

Você pode adicionar scripts no Unified Manager e associá-los a alertas. Esses scripts são executados automaticamente quando um alerta é gerado e permitem que você obtenha 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, o Perl deve ser instalado no servidor Unified Manager. Para instalações do VMware, o Perl 5 é instalado por padrão e os scripts suportarão 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 seu script criar arquivos de log para rastrear o progresso do script de alerta, você deverá garantir que os arquivos de log não sejam criados em nenhum lugar dentro da pasta de instalação do Unified Manager.

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode carregar scripts personalizados e coletar detalhes do evento sobre o alerta.



Se você não vir esse recurso disponível na interface do usuário, é porque a funcionalidade foi desabilitada pelo seu administrador. Se necessário, você pode habilitar essa funcionalidade em **Gerenciamento de armazenamento > Configurações de recursos**.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Scripts**.
2. Na página **Scripts**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar script**, clique em **Procurar** para selecionar seu arquivo de script.
4. Insira uma descrição para o script que você selecionar.
5. Clique em **Adicionar**.

Informações relacionadas

["Habilitando e desabilitando a capacidade de fazer upload de scripts"](#)

Excluir scripts

Você pode excluir um script do Unified Manager quando ele não for mais necessário ou válido.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- O script não deve ser 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 você deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

Execução do script de teste

Você pode verificar se seu script é executado corretamente quando um alerta é gerado para um objeto de armazenamento.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos 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...
Adicionar um alerta	a. Clique em Adicionar. b. Na seção Ações, associe o alerta ao seu script de teste.
Editar um alerta	a. Selecione um alerta e clique em Editar. b. Na seção Ações, associe o alerta ao seu script de teste.

5. Clique em **Salvar**.
6. Na página **Configuração de alerta**, selecione o alerta que você adicionou ou modificou e clique em **Testar**.

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.

Comandos CLI do Unified Manager suportados

Como administrador de armazenamento, você pode usar os comandos da CLI para executar consultas nos objetos de armazenamento; 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 ONTAP . Você também pode usar comandos CLI em scripts que são executados no início ou no final de uma operação ou são executados quando um alerta é acionado.

Todos os comandos devem ser precedidos pelo 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
<code>um cli login -u <username> [-p <password>]</code>	Efetua login na CLI. Por questões de segurança, você deve inserir somente o nome de usuário após a opção "-u". Quando usado dessa maneira, você será solicitado a inserir a senha, e ela não será capturada no histórico ou na tabela de processos. A sessão expira após três horas a partir do momento do login, após o qual o usuário deve efetuar login novamente.	Exibe a mensagem correspondente.
<code>um cli logout</code>	Efetua 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 <timeout>] <cluster> <command></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 de tempo máximo (em segundos) para o comando ser concluído no cliente. O padrão é 0 (esperar para sempre).	Conforme recebido da ONTAP.
<code>um run query <sql command></code>	Executa uma consulta SQL. Somente consultas que leem do banco de dados são permitidas. Nenhuma operação de atualização, inserção ou exclusão é suportada.	Os resultados são exibidos em forma de tabela. Se um conjunto vazio for retornado, ou se houver algum erro de sintaxe ou solicitação incorreta, ele exibirá a mensagem de erro apropriada.

Comando CLI	Descrição	Saída
um datasource add -u <username> -P <password> [-t <protocol>] [-p <port>] <hostname-or-ip>	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 comunicação com o cluster. Se a porta não for especificada, o valor padrão do protocolo apropriado será tentado. Este comando pode ser executado somente pelo administrador de armazenamento.	Solicita que o usuário aceite o certificado e imprime a mensagem correspondente.
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. Pode ser executado somente 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.

Comando CLI	Descrição	Saída
<code>um option set <option-name>=<option-value> [<option-name>=<option-value> ...]</code>	Define uma ou mais opções. O comando pode ser executado somente pelo administrador de armazenamento.	Exibe a mensagem correspondente.
<code>um version</code>	Exibe a versão do software Unified Manager.	<code>Version ("9.6")</code>
<code>um lun list [-q] [-ObjectType <object-id>]</code>	Lista os LUNs após filtrar o objeto especificado. -q é aplicável para todos os comandos para não mostrar nenhum cabeçalho. ObjectType pode ser lun, qtree, cluster, volume, quota ou svm. Por exemplo: <code>um lun list -cluster 1</code> Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os LUNs dentro do cluster com ID 1.	Exibe os seguintes valores em formato tabular: ID and LUN path.
<code>um svm list [-q] [-ObjectType <object-id>]</code>	Lista as VMs de armazenamento após filtrar pelo objeto especificado. ObjectType pode ser lun, qtree, cluster, volume, quota ou svm. Por exemplo: <code>um svm list -cluster 1</code> 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.	Exibe os seguintes valores em formato tabular: Name and Cluster ID.

Comando CLI	Descrição	Saída
um qtree list [-q] [-ObjectType <object-id>]	Lista as qtrees após filtrar pelo objeto especificado. -q é aplicável para todos os comandos para não mostrar nenhum cabeçalho. ObjectType pode ser lun, qtree, cluster, volume, quota ou svm. Por exemplo: um qtree list -cluster 1 Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todas as qtrees dentro do cluster com ID 1.	Exibe os seguintes valores em formato tabular: Qtree ID and Qtree Name.
um disk list [-q] [-ObjectType <object-id>]	Lista os discos após filtrar pelo objeto especificado. ObjectType pode ser disco, aggr, nó ou cluster. Por exemplo: um disk list -cluster 1 Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os discos dentro do cluster com ID 1.	Exibe os seguintes valores em formato tabular ObjectType and object-id.
um cluster list [-q] [-ObjectType <object-id>]	Lista os clusters após filtrar pelo objeto especificado. ObjectType pode ser disco, aggr, nó, cluster, lun, qtree, volume, quota ou svm. Por exemplo: um cluster list -aggr 1 Neste exemplo, "-aggr" é o objectType e "1" é o objectId. O comando lista o cluster ao qual o agregado com ID 1 pertence.	Exibe os seguintes valores em formato tabular: Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.

Comando CLI	Descrição	Saída
<pre>um cluster node list [-q] [-ObjectType <object-id>]</pre>	Lista os nós do cluster após filtrar pelo objeto especificado. ObjectType pode ser disco, aggr, nó ou cluster. Por exemplo: <pre>um cluster node list -cluster 1</pre> Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os nós dentro do cluster com ID 1.	Exibe os seguintes valores em formato tabular Name and Cluster ID.
<pre>um volume list [-q] [-ObjectType <object-id>]</pre>	Lista os volumes após filtrar pelo objeto especificado. ObjectType pode ser lun, qtree, cluster, volume, quota, svm ou aggregate. Por exemplo: <pre>um volume list -cluster 1</pre> Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os volumes dentro do cluster com ID 1.	Exibe os seguintes valores em formato tabular Volume ID and Volume Name.
<pre>um quota user list [-q] [-ObjectType <object-id>]</pre>	Lista os usuários da cota após filtrar pelo objeto especificado. ObjectType pode ser qtree, cluster, volume, quota ou svm. Por exemplo: <pre>um quota user list -cluster 1</pre> 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.	Exibe os seguintes valores em formato tabular ID, Name, SID and Email.

Comando CLI	Descrição	Saída
<code>um aggr list [-q] [-ObjectType <object-id>]</code>	Lista os agregados após filtrar o objeto especificado. ObjectType pode ser disco, aggr, nó, cluster ou volume. Por exemplo: um aggr list -cluster 1 Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os agregados dentro do cluster com ID 1.	Exibe os seguintes valores em formato tabular Aggr ID, and Aggr Name .
<code>um event ack <event-ids></code>	Reconhece um ou mais eventos.	Exibe a mensagem correspondente.
<code>um event resolve <event-ids></code>	Resolve um ou mais eventos.	Exibe a mensagem correspondente.
<code>um event assign -u <username> <event-id></code>	Atribui um evento a um usuário.	Exibe a mensagem correspondente.
<code>um event list [-s <source>] [-S <event-state-filter-list>..] [<event-id> ..]</code>	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 .
<code>um backup restore -f <backup_file_path_and_name></code>	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 que você adicione scripts ao Unified Manager.

Página de scripts

A página Scripts permite que você adicione seus scripts personalizados ao Unified Manager. Você pode associar esses scripts a alertas para habilitar a reconfiguração automática de objetos de armazenamento.

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.

Visualização de lista

A exibição de lista exibe, em formato tabular, os scripts que você adicionou ao Unified Manager.

- **Nome**

Exibe o nome do script.

- **Descrição**

Exibe a descrição do script.

Caixa de diálogo 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.

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

- **Selecione o arquivo de script**

Permite que você selecione um script para o alerta.

- **Descrição**

Permite que você especifique 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 (antigo OnCommand Unified Manager) 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 cargas de trabalho que estão usando excessivamente os componentes do cluster e diminuindo o desempenho de outras cargas de trabalho no cluster. Ao definir políticas de limite de desempenho, você também pode especificar valores máximos para determinados contadores de desempenho, para que eventos sejam gerados quando o limite for violado. O Unified Manager alerta você sobre esses eventos de desempenho para que você possa tomar medidas corretivas e trazer o desempenho de volta aos níveis normais de operação. Você pode visualizar e analisar eventos na interface do usuário do Unified Manager.

O Unified Manager monitora o desempenho de dois tipos de cargas de trabalho:

- Cargas de trabalho definidas pelo usuário

Essas cargas de trabalho consistem em volumes FlexVol e FlexGroup que você criou no seu cluster.

- Cargas de trabalho definidas pelo sistema

Essas cargas de trabalho consistem em atividades internas do sistema.

Recursos de monitoramento de desempenho do Unified Manager

O Unified Manager coleta e analisa estatísticas de desempenho 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 muitos componentes do cluster.

Um alto tempo de resposta (latência) indica que o objeto de armazenamento, por exemplo, um volume, está com desempenho mais lento 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 armazenamento onde está o problema de desempenho e fornece uma lista de ações sugeridas que você pode tomar para resolver o problema.

O Unified Manager inclui os seguintes recursos:

- Monitora e analisa estatísticas de desempenho da carga de trabalho de um sistema que executa o software ONTAP .
- Rastreia contadores de desempenho para clusters, nós, agregados, portas, SVMs, volumes, LUNs, namespaces NVMe e interfaces de rede (LIFs).
- Exibe gráficos detalhados que mostram 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 desempenho e taxa de cache.

- Permite que você crie políticas de limite de desempenho definidas pelo usuário que acionam eventos e enviam alertas por e-mail quando os limites são violados.
- Usa limites definidos pelo sistema e limites de desempenho dinâmicos que aprendem sobre sua atividade de carga de trabalho para identificar e alertá-lo sobre problemas de desempenho.
- Identifica as políticas de qualidade de serviço (QoS) e as políticas de nível de serviço de desempenho (PSLs) que são aplicadas aos seus volumes e LUNs.
- Identifica claramente o componente do cluster que está em disputa.
- Identifica cargas de trabalho que estão usando excessivamente os componentes do cluster e as cargas de trabalho cujo desempenho é afetado pelo aumento da atividade.

Interfaces do Unified Manager usadas para gerenciar o desempenho do sistema de armazenamento

Estas seções contêm informações sobre as duas interfaces de usuário que o Active IQ Unified Manager fornece para solucionar problemas de capacidade de armazenamento de dados, disponibilidade e proteção. As duas interfaces de usuário são a interface de usuário da Web do Unified Manager e o console de manutenção.

Se quiser usar os recursos de proteção no Unified Manager, você também deve instalar e configurar o OnCommand Workflow Automation (WFA).

Interface da Web do Unified Manager

A interface de usuário da Web do Unified Manager permite que um administrador monitore e solucione problemas de cluster relacionados à capacidade de armazenamento de dados, disponibilidade e proteção.

Estas seções descrevem alguns fluxos de trabalho comuns que um administrador pode seguir para solucionar problemas de capacidade de armazenamento, disponibilidade de dados ou proteção exibidos na interface do usuário da Web do Unified Manager.

Console de manutenção

O console de manutenção do Unified Manager permite que um administrador monitore, diagnostique e resolva 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 interface de usuário 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-las para resolver problemas relacionados ao funcionamento do servidor do Unified Manager.

Configuração de cluster e atividade de coleta de dados de desempenho

O intervalo de coleta de *dados de configuração do cluster* é de 15 minutos. Por exemplo, depois de adicionar um cluster, leva 15 minutos para exibir os detalhes do cluster na interface do usuário do Unified Manager. Esse intervalo também se aplica ao fazer alterações em um cluster.

Por exemplo, se você adicionar dois novos volumes a uma SVM em um cluster, verá esses novos objetos na interface do usuário após o próximo intervalo de pesquisa, 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 desempenho histórico de cinco minutos e 180 dias de dados de desempenho histórico de uma hora. Isso permite que você visualize detalhes de desempenho muito granulares do mês atual e tendências gerais de desempenho de 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 coleta que o Unified Manager executa:

Atividade	Intervalo de tempo	Descrição
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 for violado, o Unified Manager gera eventos e envia e-mails para usuários especificados, se configurado para isso.
Enquete de configuração	A cada 15 minutos	Coleta informações detalhadas de inventário de cada cluster para identificar todos os objetos de armazenamento (nós, SVMs, volumes e assim por diante).
Resumo	A cada hora	Resume as últimas 12 coletas de dados de desempenho de cinco minutos em médias horárias. Os valores médios horários são usados em algumas páginas da interface do usuário e são mantidos por 180 dias.
Análise de previsão e poda de dados	Todos os dias depois da meia-noite	Analisa dados de cluster para estabelecer limites dinâmicos para latência de volume e IOPS para as 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
Poda de dados	Todos os dias depois das 2 da manhã	Exclui do banco de dados quaisquer eventos com mais de 180 dias e limites dinâmicos com mais de 180 dias.
Poda de dados	Todos os dias depois das 3h30	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 é possível coletar dados em tempo real.

O Unified Manager realiza pesquisas de coleta de continuidade de dados de desempenho histórico quando ocorrem os seguintes eventos:

- Um cluster é adicionado inicialmente 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 ele ser adicionado.

Além disso, eventos de limite definidos pelo sistema são relatados para o período anterior, se houver algum.

- O ciclo atual de coleta de dados de desempenho não termina no prazo.

Se a pesquisa de desempenho em tempo real ultrapassar o período de coleta de cinco minutos, um ciclo de coleta de continuidade de dados será iniciado para reunir as informações ausentes. Sem a coleta de continuidade de dados, o próximo período de coleta é ignorado.

- O Unified Manager fica inacessível por um período de tempo e depois volta a ficar online, como nas seguintes situações:
 - Foi reiniciado.
 - Ele foi desligado durante uma atualização de software ou ao criar um arquivo de backup.
 - Uma interrupção de rede é reparada.
- Um cluster fica inacessível por um período de tempo e depois volta a ficar online, como nas seguintes situações:
 - Uma interrupção de rede é reparada.
 - Uma conexão lenta de rede de longa distância 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 ficar inativo por mais de 24 horas, uma lacuna nos dados de desempenho aparecerá nas páginas da interface do usuário.

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 o registro de data e hora significa em dados e eventos coletados

O registro de data e hora que aparece nos dados de desempenho e integridade coletados, ou que aparece como o horário de detecção de um evento, é baseado no horário do cluster ONTAP , ajustado ao fuso horário definido no navegador da web.

É altamente recomendável que você use um servidor Network Time Protocol (NTP) para sincronizar a hora em seus servidores do Unified Manager, clusters ONTAP e navegadores da web.



Se você vir registros de data e hora que parecem incorretos para um cluster específico, talvez seja necessário verificar se o horário do cluster foi definido corretamente.

Navegue pelos fluxos de trabalho de desempenho na GUI do Unified Manager

A interface do Unified Manager fornece muitas páginas para coleta e exibição de informações de desempenho. Use o painel de navegação esquerdo para navegar até as páginas da GUI e use guias e links nas páginas para visualizar e configurar informações.

Use todas as páginas a seguir para monitorar e solucionar problemas de informações de desempenho do cluster:

- página do painel
- 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 instalação
- páginas de eventos

Efetue login na interface do usuário

Você pode efetuar login na interface do usuário do Unified Manager usando um navegador da Web compatível.

Antes de começar

- O navegador da web deve atender aos requisitos mínimos.

Veja a Matriz de Interoperabilidade em ["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix) para obter a lista completa de versões de navegadores 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 pode ser configurado em **Geral > Configurações de recursos**.

Passos

1. Insira a URL no seu 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. . Na tela de login, digite seu nome de usuário e senha.

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.

A página Painel é exibida.



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 manipulará as comunicações por e-mail e se o AutoSupport está habilitado para enviar informações sobre sua instalação do Unified Manager ao suporte técnico. A interface do usuário do Unified Manager aparece depois que você preenche essas informações.

Interface gráfica e caminhos de navegação

O Unified Manager tem grande flexibilidade e permite que você realize diversas tarefas de diversas maneiras. Há muitos caminhos de navegação que você descobrirá ao trabalhar 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 armazenamento fornece uma visão geral do desempenho do cluster e do objeto e inclui o monitoramento de eventos de desempenho. Você pode visualizar o desempenho e os eventos em alto nível ou pode investigar mais detalhes sobre o desempenho do objeto e os eventos de desempenho.

Este é um exemplo de muitas possíveis navegações de objetos de cluster:

1. Na página Painel, revise os detalhes no painel Capacidade de desempenho para identificar o cluster que está usando a maior capacidade de desempenho e clique no gráfico de barras para navegar até a lista de nós desse cluster.

2. Identifique o nó com o maior valor de capacidade de desempenho utilizado e clique nesse nó.
3. Na página Node/Desempenho Explorer, clique em **Agregados neste nó** no menu Exibir e comparar.
4. Identifique o agregado que está usando a maior capacidade de desempenho e clique nele.
5. Na página Agregado/Explorador de Desempenho, clique em **Volumes neste Agregado** no menu Exibir e Comparar.
6. Identifique os volumes que estão usando mais IOPS.

Você deve investigar esses volumes para ver se deve aplicar uma política de QoS ou uma política de Nível de Serviço de Desempenho, ou alterar as configurações da política, para 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...licity	40.5 TB	< 1 month	13.0:1
umeng...1-02	83.6 TB	51 days	8.0:1
sysmgr...0-1-8	33 TB	143 days	6.3:1

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...	5.8 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
suchita_vmware_d...	6.38 ms...	76.8 IOPS	2.55 MB/s
suchita_vmware_d...	3.82 ms...	4,775 L...	16.7 MB/s
aiqum_scale_do_no...	0.114 m...	< 1 IOPS	< 1 MB/s

Monitorar a navegação de desempenho do cluster

Você pode monitorar o desempenho de todos os clusters gerenciados pelo Unified Manager. O monitoramento de seus clusters fornece uma visão geral do desempenho do cluster e do objeto e inclui o monitoramento de eventos de desempenho. Você pode visualizar o desempenho e os eventos em alto nível ou pode investigar mais detalhadamente quaisquer detalhes do desempenho do cluster e do objeto, bem como dos eventos de desempenho.

Este é um exemplo dos muitos caminhos possíveis de navegação de desempenho de cluster:

1. No painel de navegação esquerdo, clique em **Armazenamento > Agregados**.
2. Para visualizar informações sobre o desempenho desses agregados, selecione a visualização Desempenho: Todos os agregados.
3. Identifique o agregado que você deseja investigar e clique no nome dele para navegar até a página Aggregate / Performance Explorer.
4. Opcionalmente, selecione outros objetos para comparar com este agregado no menu Exibir e Comparar e adicione um dos objetos ao painel de comparação.

Estatísticas para ambos os objetos aparecerão nos gráficos de contagem para comparação.

5. No painel Comparação, à direita na página do Explorer, clique em **Visualização com Zoom** em um dos gráficos de contadores para visualizar 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	Latency	IOPS	MB/s	Perf...
aggr3	5.06 ...	3.06 ...	< 1 M...	6%
aggr_evt	0.29 ...	3.79 ...	< 1 M...	< 1%
aggr_automation	0.27 ...	6.35 ...	< 1 M...	< 1%

Comparing

1 Additional Object

X

aggr4

aggr3

CHOOSE CHARTS 7 Charts Selected

Events for Aggregate: aggr4



No data to display

Latency

VIEW Total

Zoom View

Latency - Total view (ms/op)



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

25 ms/op

20

15

10

5

0

Latency - Total view (ms/op)

aggr4

aggr3

Nov 14, 2019, 1:24 AM

4.25

3.97

Nov 15, 2019, 12:00 AM Nov 15, 2019, 12:00 PM Nov 14, 2019, 12:00 AM Nov 14, 2019, 12:00 PM Nov 15, 2019, 12:00 AM Nov 15, 2019, 12:00 PM

Navegação de investigação de eventos

As páginas de detalhes do evento do Unified Manager fornecem uma visão detalhada de qualquer evento de apresentação. Isso é benéfico ao investigar eventos de desempenho, ao solucionar problemas e ao ajustar o desempenho do sistema.

Dependendo do tipo de evento de performance, você poderá ver um dos dois tipos de páginas de detalhes do evento:

- Página de detalhes do evento para eventos de política de limite definidos pelo usuário e 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 ativos**.
3. Clique no nome do evento que você deseja investigar e a página Detalhes do evento será exibida.
4. Veja a Descrição do evento e revise as Ações sugeridas (quando disponíveis) para ver mais detalhes sobre o evento que podem ajudar você a resolver o problema. Você pode clicar no botão **Analisar carga de trabalho** para exibir gráficos de desempenho detalhados para ajudar a analisar melhor o problema.

Event Management

Last updated: Nov 15, 2019, 11:23 AM

VIEW

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		New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs2:/julia_feb12_vol1	Volume
Nov 14, 2019, 11:39 AM		New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs7:/julia_non_shared_3	Volume
Nov 15, 2019, 5:04 AM		New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	suchita_vmwvar...nt_delete_01	Volume
Nov 15, 2019, 10:39 AM		New	Risk	Performance	Workload LUN Latency ...Service Level Policy	iscsi_boot/ia.../ocum-c220-01	LUN
Nov 15, 2019, 10:39 AM		New	Risk	Performance	Workload LUN Latency ...Service Level Policy	iscsi_boot/ia.../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	ION 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

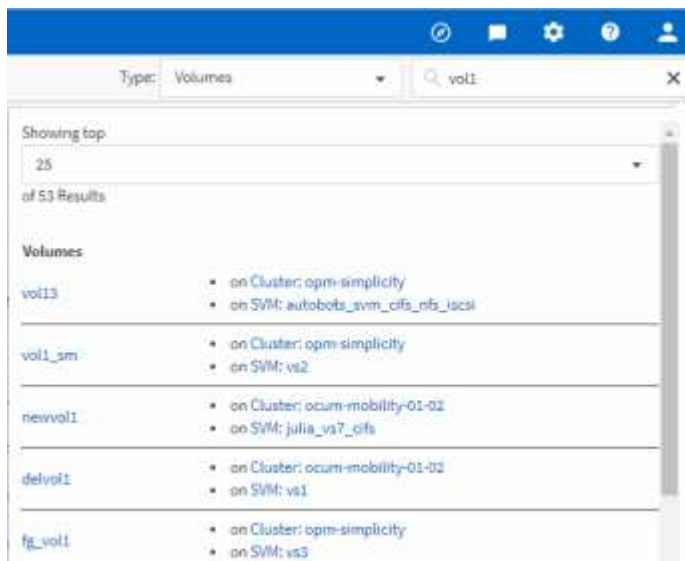
Pesquisar objetos de armazenamento

Para acessar rapidamente um objeto específico, você pode usar o campo **Pesquisar todos os objetos de armazenamento** na parte superior da barra de menu. Este método de pesquisa global em todos os objetos permite que você localize 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 principais resultados da pesquisa são acessíveis. Por isso, a funcionalidade de pesquisa global pode ser considerada uma ferramenta de atalho para encontrar itens específicos, se você souber quais itens 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 **Todos** para pesquisar simultaneamente em todos os objetos e eventos. Como alternativa, você pode clicar na caixa suspensa para especificar o tipo de objeto. Digite no mínimo 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 clusters
- Nós: nomes dos nós
- Agregados: nomes de agregados
- SVMs: nomes de SVM
- Volumes: nomes dos volumes
- LUNs: caminhos de LUN



LIFs e portas não podem ser pesquisados 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 da pesquisa para navegar até 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.

Filtrar conteúdo da página de inventário

Você pode filtrar dados da página de inventário no Unified Manager para localizar dados rapidamente com base em critérios específicos. Você pode usar a filtragem para restringir o conteúdo das páginas do Unified Manager e 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 **Filtragem** para personalizar a visualização em grade com base em suas preferências. As opções de filtro disponíveis são baseadas no tipo de objeto visualizado na grade. Se filtros estiverem aplicados no momento, o número de filtros aplicados será exibido à direita do botão Filtro.

Três tipos de parâmetros de filtro são suportados.

Parâmetro	Validação
String (texto)	Os operadores são contém , começa com , termina com e não contém .
Número	Os operadores são maior que , menor que , no último e entre .
Enum (texto)	Os operadores são is e is not .

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 quatro. Os resultados filtrados são baseados em parâmetros de filtro combinados. Os resultados filtrados se aplicam a todas as páginas da sua pesquisa filtrada, não apenas à página exibida no momento.

Você pode adicionar filtros usando o painel Filtragem.

1. No topo da página, clique no botão **Filtro**. O painel Filtragem é exibido.
2. Clique na lista suspensa à esquerda e selecione um objeto; por exemplo, *Cluster* ou um contador de desempenho.
3. Clique na lista suspensa central e selecione o operador que deseja usar.
4. Na última lista, selecione ou insira um valor para completar o filtro para aquele objeto.
5. Para adicionar outro filtro, clique em **+Adicionar filtro**. Um campo de filtro adicional é exibido. Complete este filtro usando o processo descrito nas etapas anteriores. Observe que ao adicionar seu quarto filtro, o botão **+Adicionar Filtro** não será mais exibido.
6. Clique em **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 **Redefinir** 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](#)

[Cancel](#) [Apply Filter](#)

Após clicar em **Aplicar filtro**, o painel Filtragem fecha, aplica seus filtros e mostra o número de filtros aplicados (3).

Monitore o desempenho do cluster no Painel

O Painel do Unified Manager fornece alguns painéis que exibem o status de desempenho de alto nível de todos os clusters monitorados por esta instância do Unified Manager. Ele permite que você avalie o desempenho geral dos clusters gerenciados e anote, localize ou atribua rapidamente para resolução quaisquer eventos específicos identificados.

Entenda os painéis de desempenho no Dashboard

O Painel do Gerenciador Unificado fornece alguns painéis que exibem o status de desempenho de alto nível para todos os clusters que estão sendo monitorados em seu ambiente. Você pode escolher visualizar 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 naquela categoria e o número de novos eventos adicionados nas últimas 24 horas. Essas informações ajudam você a decidir quais clusters você pode precisar analisar mais detalhadamente para resolver os 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 naquela categoria.

Os painéis a seguir fornecem o status de desempenho.

- **Painel de Capacidade de Desempenho**

Ao visualizar todos os clusters, este painel exibe o valor da capacidade de desempenho de cada cluster (média da última hora) 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 para a página de inventário de nós daquele cluster. Observe que a página de inventário de nós exibe a capacidade de desempenho média das últimas 72 horas, portanto, esse valor pode não corresponder ao valor do Painel.

Ao visualizar um único cluster, este painel exibe a capacidade de desempenho do cluster, o IOPS total e os valores de taxa de transferência total.

- **Painel de carga de trabalho IOPS**

Quando o gerenciamento ativo da carga de trabalho está habilitado e ao visualizar um único cluster, este

painel exibe o número total de cargas de trabalho que estão sendo executadas em um determinado intervalo de IOPS.

- **Painel de desempenho da carga de trabalho**

Quando o gerenciamento ativo da carga de trabalho está habilitado, este painel exibe o número total de cargas de trabalho em conformidade e não em conformidade atribuídas a cada Nível de Serviço de Desempenho 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 visualizá-los classificados pelo maior IOPS ou taxa de transferência (MB/s).

Ao visualizar um único cluster, você pode optar por visualizar as cargas de trabalho nesse cluster classificados pelo maior IOPS ou taxa de transferência (MB/s).

Mensagens e descrições de banners de desempenho

O Unified Manager pode exibir mensagens de banner na página Notificações (do 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 foi interrompido e nenhum dado de desempenho está sendo coletado de nenhum cluster.	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 em execução 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 coletados após a conclusão do ciclo de coleta de continuidade de dados. Um ciclo de coleta de continuidade de dados é executado quando um novo cluster é adicionado ou quando o Unified Manager não consegue 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 perceber que as coletas de clusters grandes não estão terminando dentro do tempo padrão. Esta configuração afeta a coleta de estatísticas de todos os clusters que esta instância do Unified Manager está

monitorando.

Antes de começar

Você deve ter um ID de usuário e uma senha autorizados para efetuar login no console de manutenção do servidor do Unified Manager.

O problema das coletas de estatísticas de desempenho não serem concluídas no prazo é indicado 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 configuração por nenhum outro motivo.



Alterar esse valor da configuração padrão de 5 minutos pode afetar o número e a frequência de eventos de desempenho relatados pelo Unified Manager. Por exemplo, limites de desempenho definidos pelo sistema acionam eventos quando a política é excedida por 30 minutos. Ao utilizar coletas de 5 minutos, a política deve ser excedida por seis coletas consecutivas. Para coletas 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 atual de coleta de dados estatísticos.

Passos

1. Efetue login usando SSH como 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 rotulada **Configuração do intervalo de pesquisa de desempenho** e pressione Enter.
3. Se solicitado, digite a senha do usuário de manutenção novamente.
4. Digite o número do novo intervalo de pesquisa que você deseja definir e pressione Enter.

Se você alterou o intervalo de coleta do Unified Manager para 10 ou 15 minutos e tem uma conexão atual com um provedor de dados externo (como o Graphite), você deve alterar o intervalo de transmissão do provedor de dados para que seja igual ou maior que o intervalo de coleta do Unified Manager.

Solucionar 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 auxiliar na solução de problemas. Ao visualizar todos os eventos atuais e passados de uma carga de trabalho, você pode ter uma ideia melhor do motivo pelo qual a carga de trabalho pode estar tendo um problema de desempenho ou capacidade agora.

Usar essa ferramenta também pode ajudar a determinar se o armazenamento é a causa de algum problema de desempenho de um aplicativo ou se o problema é causado por um problema de rede ou outro problema relacionado.

Você pode iniciar essa funcionalidade de vários lugares na interface do usuário:

- Na seleção **Análise de Carga de Trabalho** no menu de navegação à esquerda
- Na página de detalhes do evento, clicando no botão **Analisar carga de trabalho**
- Em qualquer página de inventário de carga de trabalho (volume, LUN, carga de trabalho, compartilhamento NFS ou compartilhamento SMB/CIFS), clicando no ícone mais , então **Analisar Carga de Trabalho**
- Na página Máquinas Virtuais, clicando no botão **Analisar Carga de Trabalho** de qualquer objeto 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. Ao iniciar a ferramenta em qualquer uma das páginas de carga de trabalho ou inventário de 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. Ao iniciar a ferramenta na página 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 potencialmente corrigir o problema que está causando 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 durante o qual deseja ver estatísticas. Você pode alterar o período de tempo a qualquer momento se quiser visualizar 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 carga de trabalho para LUNs não fornecem o mesmo nível de estatísticas que os gráficos para volumes, portanto, você notará diferenças ao analisar esses dois tipos de cargas de trabalho.

• Área de resumo de eventos

Exibe uma breve visão geral do número e dos tipos de eventos que ocorreram ao longo do período. Quando há eventos de diferentes áreas de impacto (por exemplo, desempenho e capacidade), essas informações são exibidas para que você possa selecionar detalhes para o tipo de evento no qual está interessado. Clique no tipo de evento para visualizar uma lista dos nomes dos eventos.

Se houver apenas um evento durante o período, uma lista de recomendações para corrigir o problema será listada para alguns eventos.

• Cronograma do evento

Mostra todas as ocorrências de eventos durante o período especificado. Passe o cursor sobre cada evento para ver o nome do evento.

Se você chegou a esta página clicando no botão **Analisar carga de trabalho** na página Detalhes do evento, o ícone do evento selecionado aparecerá maior para que você possa identificá-lo.

• Área de gráficos de desempenho

Exibe gráficos de latência, taxa de transferência (IOPS e MB/s) e utilização (para o nó e o agregado) com base no período selecionado. Você pode clicar no link Exibir detalhes de desempenho para exibir a página do Performance Explorer da carga de trabalho, caso queira realizar análises mais detalhadas.

- **Latência** exibe a latência da carga de trabalho durante o período selecionado. O gráfico tem três visualizações que permitem que você veja:
 - Latência **Total**
 - Latência de **detalhamento** (dividida por leituras, gravações e outros processos)
 - Latência dos **Componentes do Cluster** (dividida por componente do cluster)

Ver "[Componentes do cluster e por que eles podem estar em disputa](#)" para uma descrição dos componentes do cluster que são exibidos aqui. **Throughput exibe a taxa de transferência de IOPS e MB/s para a carga de trabalho durante o período selecionado. O gráfico tem quatro visualizações que permitem que você veja:** * Taxa de transferência **Total** * Taxa de transferência **Detalhada (dividida por leituras, gravações e outros processos)** * Taxa de transferência **na nuvem** (os MB/s usados para gravar e ler dados na nuvem; para as cargas de trabalho que estão escalonando a capacidade para a nuvem) * **IOPS com previsão (uma previsão de quais eram os valores de taxa de transferência de IOPS superior e inferior esperados ao longo do período)** Este gráfico também exibe as configurações de limite de taxa de transferência máxima e mínima de Qualidade de Serviço (QoS), se configuradas, para que você possa ver onde o sistema pode estar limitando a taxa de transferência intencionalmente com políticas de QoS. **Utilização** exibe a utilização do agregado e do nó no qual a carga de trabalho está sendo executada durante o período selecionado. A partir daqui, você pode ver se seu agregado ou nó está sendo superutilizado, possivelmente causando alta latência. Ao analisar volumes do FlexGroup, há vários nós e vários agregados listados nos gráficos de utilização.

• Área do gráfico de capacidade

Exibe gráficos de capacidade de dados e capacidade de instantâneo do último mês para a carga de trabalho.

Para volumes, você pode clicar no link Exibir detalhes de 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 uma página de Detalhes de integridade para LUNs.

- **Capacity View** exibe o espaço total disponível alocado para a carga de trabalho e o espaço lógico usado (após todas as otimizações do NetApp).
- **Visualização de instantâneo** exibe o espaço total reservado para cópias de instantâneo e a quantidade de espaço que está sendo usada no momento. Observe que os LUNs não fornecem uma Visualização de Instantâneo.
- **Cloud Tier View** exibe quanta capacidade está sendo usada no nível de desempenho local e quanta está sendo usada no nível de nuvem. Esses gráficos incluem uma estimativa da quantidade de tempo restante antes que a capacidade dessa carga de trabalho esteja cheia. Essas informações são baseadas no uso histórico e exigem no mínimo 10 dias de dados. Quando restam menos de 30 dias de capacidade, o Unified Manager identifica o armazenamento como “quase cheio”.

Quando devo usar o analisador de 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 está operando de

forma anormal.

Caso os usuários tenham entrado em contato com você para dizer que o aplicativo que estão usando está muito lento, você pode verificar os gráficos de latência, taxa de transferência e utilização da carga de trabalho na qual o aplicativo está sendo executado para ver se o armazenamento é a causa do problema de desempenho. Você também pode usar o gráfico de capacidade para verificar se a capacidade está baixa, pois um sistema ONTAP em que a capacidade é utilizada em mais de 85% pode causar problemas de desempenho. Esses gráficos ajudarão você a determinar se o problema é causado pelo armazenamento, pela rede ou por outro problema relacionado.

Caso o Unified Manager tenha gerado um evento de desempenho e você queira analisar a causa do problema mais detalhadamente, você pode iniciar o analisador de carga de trabalho na página Detalhes do evento clicando no botão **Analisar carga de trabalho** para pesquisar algumas tendências de latência, taxa de transferência e capacidade da carga de trabalho.

Caso você perceba uma carga de trabalho que parece estar operando de forma anormal 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  , então **Analisar carga de trabalho** para abrir a página Análise de carga de trabalho para examinar a carga de trabalho mais detalhadamente.

Use 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 como iniciar a ferramenta a partir do painel de navegação esquerdo.

Passos

1. No painel de navegação esquerdo, clique em **Análise de carga de trabalho**.

A página Análise de carga de trabalho é exibida.

2. Se você souber o nome da carga de trabalho, insira-o. Se você não tiver certeza do nome completo, insira no mínimo 3 caracteres e o sistema exibirá uma lista de cargas de trabalho que correspondem à sequência de caracteres.
3. Selecione o intervalo de tempo se quiser visualizar estatísticas por mais tempo do que o padrão de 2 horas e clique em **Aplicar**.
4. Visualize a área Resumo para ver os eventos que ocorreram durante o período.
5. Veja os gráficos de desempenho e capacidade para ver quando alguma das métricas está anormal e veja se algum evento se alinha com a entrada anormal.

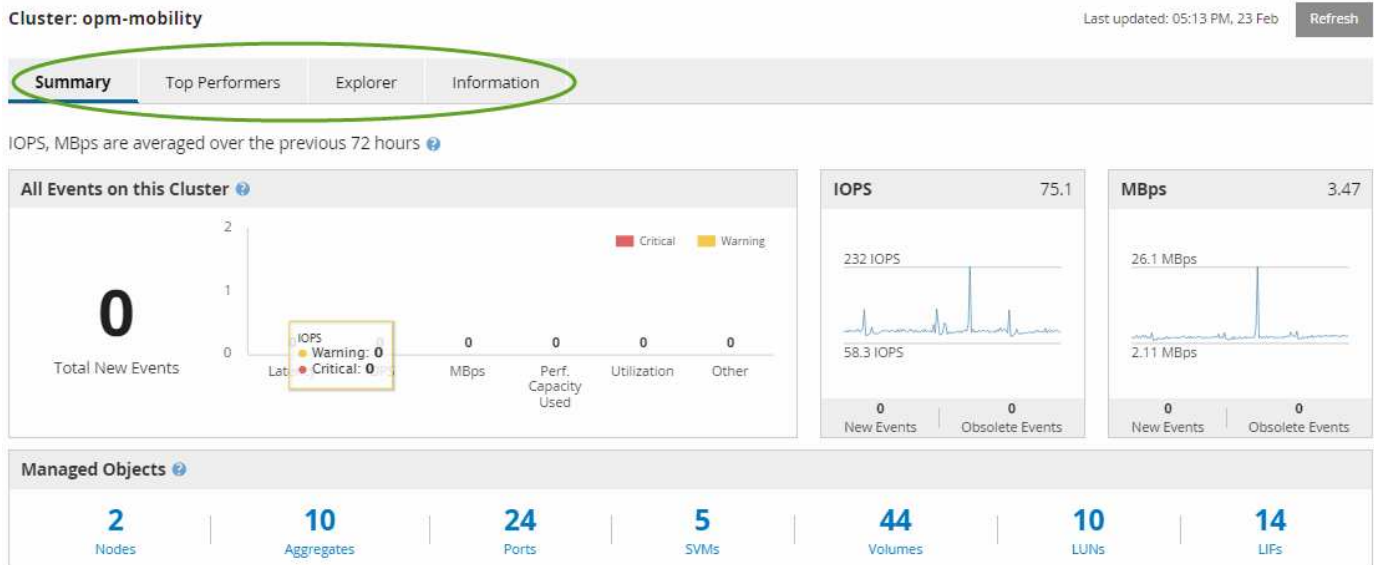
Monitore o desempenho do cluster na página inicial do Performance Cluster

A página inicial 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 que você avalie o desempenho geral de um cluster específico e observe, localize ou atribua rapidamente para resolução quaisquer eventos específicos do cluster que sejam identificados.

Entenda a página de destino do cluster de desempenho

A página inicial do cluster de desempenho fornece uma visão geral de alto nível do desempenho de um cluster selecionado, com ênfase no status de desempenho dos 10 principais objetos dentro do cluster. Problemas de desempenho são exibidos na parte superior da página, no painel Todos os eventos neste cluster.

A página inicial 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 desempenho e permite monitorar e solucionar problemas de clusters. A imagem a seguir mostra um exemplo da página inicial do Performance Cluster 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 em cada uma das barras 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 política de combinação foi violada.



Se um cluster foi removido do gerenciamento pelo Unified Manager, o status **Removido** é exibido à direita do nome do cluster, na parte superior da página.

Página de destino do cluster de desempenho

A página inicial do cluster de desempenho exibe o status de desempenho de alto nível de um cluster selecionado. A página permite que você acesse detalhes completos de cada contador de desempenho para os objetos de armazenamento no cluster selecionado.

A página inicial do Cluster de Desempenho inclui quatro guias que separam os detalhes do cluster em quatro áreas de informações:

- Página de resumo
 - Painel Eventos de Cluster

- Gráficos de desempenho de MB/s e IOPS
- Painel Objetos Gerenciados
- Página dos Melhores Desempenhos
- Página do Explorer
- Página de informações

Página Resumo do Cluster de Desempenho

A página Resumo do cluster de desempenho fornece um resumo dos eventos ativos, desempenho de IOPS e desempenho de MB/s para um cluster. Esta página também inclui a contagem total de objetos de armazenamento no cluster.

Painel de eventos de desempenho do cluster

O painel Eventos de desempenho do cluster exibe estatísticas de desempenho e todos os eventos ativos do cluster. Isso é muito útil ao monitorar seus clusters e todo o desempenho e eventos relacionados a eles.

Todos os eventos neste painel de cluster

O painel Todos os eventos neste cluster exibe todos os eventos de desempenho do cluster ativo nas últimas 72 horas. O Total de Eventos Ativos é exibido na extrema esquerda; esse número representa o total de todos os eventos Novos e Confirmados para todos os objetos de armazenamento neste cluster. Você pode clicar no link Total de eventos ativos para navegar até a página Inventário de eventos, que é filtrada para exibir esses eventos.

O gráfico de barras Total de Eventos Ativos do cluster exibe o número total de eventos críticos e de aviso ativos:

- Latência (total para nós, agregados, SVMs, volumes, LUNs e namespaces)
- IOPS (total para clusters, nós, agregados, SVMs, volumes, LUNs e namespaces)
- MB/s (total para clusters, nós, agregados, SVMs, volumes, LUNs, namespaces, portas e LIFs)
- Capacidade de desempenho utilizada (total para nós e agregados)
- Utilização (total para nós, agregados e portas)
- Outros (taxa de perda 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 verticais do contador) são exibidos em vermelho (■) para eventos críticos e amarelo (■) para eventos de alerta. Posicione o cursor sobre cada barra vertical do contador para visualizar o tipo e o número real de eventos. Você pode clicar em **Atualizar** para atualizar os dados do painel do contador.

Você pode mostrar ou ocultar eventos críticos e de aviso no gráfico de desempenho Total de Eventos Ativos clicando nos ícones **Crítico** e **Aviso** na legenda. Se você ocultar determinados tipos de eventos, os ícones de legenda serão exibidos em cinza.

Painéis de balcão

Os painéis de contadores exibem a atividade do cluster e os eventos de desempenho das 72 horas anteriores e incluem os seguintes contadores:

- **Painel de contador IOPS**

IOPS indica a velocidade operacional do cluster em número de operações de entrada/saída por segundo. Este painel de contador fornece uma visão geral de alto nível da integridade do IOPS do cluster no período anterior de 72 horas. Você pode posicionar o cursor sobre a linha de tendência do gráfico para visualizar o valor do IOPS de um período específico.

- **Painel de contagem MB/s**

MB/s indica quantos dados foram transferidos de e para o cluster em megabytes por segundo. Este painel de contador fornece uma visão geral de alto nível da integridade de MB/s do cluster no período anterior de 72 horas. Você pode posicionar o cursor sobre a linha de tendência do gráfico para visualizar o valor de 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 linha de tendência são os valores mínimo e máximo do 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 reconhecido). O problema que causou o evento não foi corrigido ou não foi resolvido. O contador de desempenho do objeto de armazenamento permanece acima do limite de desempenho.

- **Obsoleto**

Indica que o evento não está mais ativo. O problema que causou o evento foi corrigido ou resolvido. O contador de desempenho do objeto de armazenamento 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 acessar a 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 objeto selecionado.

Painel Objetos Gerenciados

O painel Objetos gerenciados na guia Resumo de desempenho fornece uma visão geral de alto nível dos tipos e contagens de objetos de armazenamento do cluster. Este painel permite que você acompanhe o status dos objetos em cada cluster.

A contagem de objetos gerenciados são dados pontuais 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 discos independentes (RAID) redundantes que podem ser gerenciados como uma única unidade para proteção e provisionamento.

- **Portas**

Um ponto de conexão física em nós que é usado para conectar a outros dispositivos em uma rede.

- **VMs de armazenamento**

Uma máquina virtual que fornece acesso à rede por meio de endereços de rede exclusivos. Uma SVM pode fornecer dados de um namespace distinto e pode ser administrada separadamente do restante 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 FlexGroup ; não inclui constituintes FlexGroup .

- **LUNs**

O identificador de uma unidade lógica Fibre Channel (FC) ou 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 de rede a um nó. A contagem inclui todos os tipos de interface.

Página dos Melhores Desempenhos

A página Melhores Desempenhos exibe os objetos de armazenamento que têm o maior ou menor desempenho, com base no contador de desempenho selecionado. Por exemplo, na categoria VMs de armazenamento, você pode exibir as SVMs que têm o maior IOPS, a maior latência ou os menores MB/s. Esta página também mostra se algum dos melhores artistas tem algum evento de performance ativo (Novo ou Reconhecido).

A página Melhores desempenhos exibe no máximo 10 de cada objeto. Observe que o objeto Volume inclui volumes FlexVol e FlexGroup .

- **Intervalo de tempo**

Você pode selecionar um intervalo de tempo para visualizar os melhores desempenhos; o intervalo de tempo selecionado se aplica a todos os objetos de armazenamento. Intervalos de tempo disponíveis:

- Última hora

- Últimas 24 horas
- Últimas 72 horas (padrão)
- Últimos 7 dias

• Métrica

Clique no menu **Métrica** para selecionar um contador diferente. As opções de contador são exclusivas para o 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:

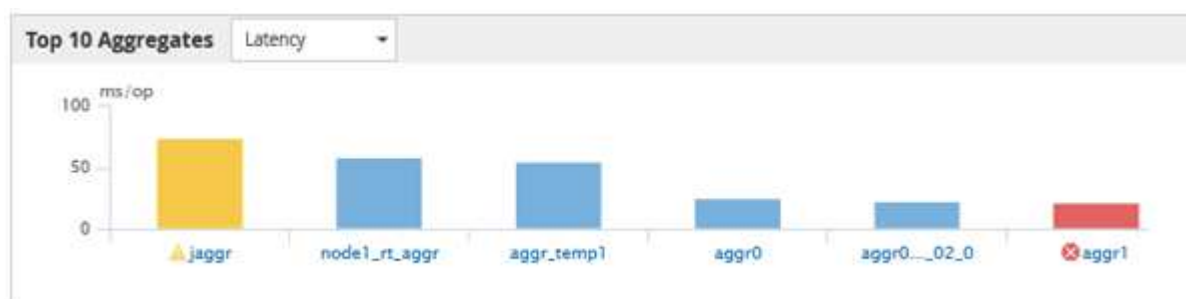
- Latência
- IOPS
- MB/s
- Capacidade de desempenho utilizada (para nós e agregados)
- Utilização (para nós e agregados)

• Organizar

Clique no menu **Classificar** para selecionar uma classificação crescente ou decrescente para o objeto e contador selecionados. As opções são **Do maior para o menor** e **Do menor para o maior**. Essas opções permitem que você visualize os objetos com o melhor ou o pior desempenho.

• Balcão

A barra do contador no gráfico mostra as estatísticas de desempenho de cada objeto, representadas como uma barra para esse item. Os gráficos de barras são codificados por cores. Se o contador não ultrapassar um limite de desempenho, a barra do contador será exibida em azul. Se uma violação de limite estiver ativa (um evento novo ou reconhecido), a barra será exibida na cor do evento: eventos de aviso serão exibidos em amarelo (■), e eventos críticos são exibidos em vermelho (■). Violações de limites são ainda indicadas por ícones indicadores de eventos de gravidade para eventos de aviso e críticos.



Para cada gráfico, o eixo X exibe os melhores desempenhos para o tipo de objeto selecionado. O eixo Y exibe unidades aplicáveis ao contador selecionado. Clicar no link do nome do objeto abaixo de cada elemento do gráfico de barras verticais navega até a página de destino de desempenho do objeto selecionado.

• Indicador de evento de gravidade

O ícone indicador **Evento de gravidade** é exibido à esquerda do nome de um objeto para eventos críticos ativos (⛔) ou aviso (⚠) eventos nos gráficos dos melhores desempenhos. Clique no ícone indicador **Evento de gravidade** para visualizar:

- **Um evento**

Navega até a página de detalhes do evento.

- **Dois ou mais eventos**

Navega até a página Inventário de eventos, que é filtrada para exibir todos os eventos do 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 cluster único que está visualizando ou para todos os clusters no data center.

Monitore o desempenho usando as páginas do Inventário de Desempenho

As páginas de desempenho do 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 rápida do status de desempenho de cada objeto dentro de um cluster, por exemplo, para todos os nós ou todos os volumes.

As páginas de desempenho do 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 de objetos, porque 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	Search Nodes	
Assign Performance Threshold Policy		Clear Performance Threshold Policy	
		Schedule Report	
☐	Status  Node	Latency	IOPS
☐	Node	MBps	Flash Cache Reads
☐	Node	Perf. Capacity Used	Utilization
☐	Node	Free Capacity	Total Capacity
☐	Node	Cluster	
☐	 ocum-mobility-02	10.2 ms/op	18,884 IOPS
☒	 opm-simplicity-01	2.01 ms/op	39,358 IOPS
☐	 ocum-mobility-01	0.018 ms/op	< 1 IOPS
☐	 opm-simplicity-02	17 ms/op	14,627 IOPS

Por padrão, os objetos nas páginas de inventário de desempenho são classificados com base na criticidade do desempenho do objeto. Objetos com novos eventos críticos de desempenho são listados primeiro, e 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 desempenho 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 de 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 sobre o objeto selecionado, incluindo comparação lado a lado de eventos ativos.

Exibir 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 desempenho sobre cada um dos objetos de armazenamento disponíveis, como clusters, agregados, volumes e assim por diante. Você pode acessar as páginas de detalhes do objeto Desempenho para visualizar informações detalhadas de um objeto específico.

Por padrão, os objetos nas páginas de exibição são classificados com base na criticidade do evento. Objetos com eventos críticos são listados primeiro, e 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 valores separados por vírgula (`.csv`) arquivo, arquivo Microsoft Excel (`.xlsx`), ou (`.pdf`) documento usando o botão **Relatórios** e, em seguida, use os dados exportados para criar relatórios. Além disso, você pode personalizar a página e agendar um relatório para ser criado e enviado por e-mail regularmente usando o botão **Relatórios agendados**.

Todos os campos nessas páginas podem ser usados em visualizações personalizadas e em relatórios. Alguns campos estão vinculados a páginas relacionadas, permitindo uma visão 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 para cada cluster monitorado por uma instância do Unified Manager. Esta página permite monitorar o desempenho dos seus clusters e solucionar problemas de desempenho e eventos de limite.

Você pode atribuir ou limpar políticas de limite de desempenho 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.

- FQDN do cluster: o nome de domínio totalmente qualificado (FQDN) do cluster.
- IOPS: 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 do cluster.
- Versão do sistema operacional: a versão do software ONTAP instalada no cluster.



Se versões diferentes do software ONTAP estiverem instaladas nos nós do cluster, o menor número de versão será listado. Você pode visualizar a versão do ONTAP instalada em cada nó na exibição Desempenho: Todos os nós.

- Política de limite: a política ou políticas de limite de desempenho definidas pelo usuário que estão ativas neste objeto de armazenamento. Você pode posicionar o cursor sobre os nomes de políticas que contêm reticências (...) para visualizar o nome completo da política ou a lista de nomes de políticas atribuídos. Os botões Atribuir política de limite de desempenho e Limpar política de limite de desempenho permanecem desabilitados até que você selecione um ou mais objetos clicando nas caixas de seleção localizadas na extrema esquerda.

Desempenho: Visualização de todos os volumes

A exibição Desempenho: Todos os volumes exibe uma visão geral dos eventos de desempenho, dados do contador e informações de configuração para cada FlexVol volume e FlexGroup que está sendo monitorado por uma instância do Unified Manager. Isso permite que você monitore rapidamente o desempenho dos seus volumes e solucione problemas de desempenho e eventos de limite.

Se você quiser analisar a latência e a taxa de transferência de um objeto específico, clique no botão mais opções  então **Analisar carga de trabalho** e você poderá visualizar gráficos de desempenho e capacidade na página Análise de carga de trabalho. Você pode visualizar os detalhes no Gerenciador de Sistemas, desde que tenha credenciais válidas para o Gerenciador de Sistemas.



Para volumes de proteção de dados (DP), somente os valores do contador para tráfego gerado pelo usuário são exibidos. Os volumes raiz não são exibidos nesta página.

A seguir estão alguns campos importantes na visualização Desempenho: Todos os volumes.

- Estilo: FlexVol ou FlexGroup.
- Latência: Para volumes FlexVol , este é o tempo médio de resposta do volume para todas as solicitações de E/S, expresso em milissegundos por operação. Para volumes FlexGroup , esta 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 fornecido por uma determinada quantidade de capacidade de armazenamento.
- IOPS: Para volumes FlexVol , este é o número de operações de entrada/saída por segundo para o volume. Para volumes FlexGroup , esta 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.

Veja os links a seguir para mais informações:

- ["Atribuindo políticas de limite de desempenho a objetos de armazenamento"](#)
- ["Removendo políticas de limite de desempenho de objetos de armazenamento"](#)
- ["Tipos de cargas de trabalho monitoradas pelo Unified Manager"](#)
- ["Visualizando as configurações do grupo de políticas de QoS aplicadas a volumes ou LUNs específicos"](#)
- ["Compreendendo as recomendações do Unified Manager para hierarquizar dados na nuvem"](#)
- ["Visualizar gráficos de desempenho para comparar volumes ou LUNs que estão no mesmo grupo de políticas de QoS"](#)

Desempenho: Visualização de todos os agregados

A exibição Desempenho: todos os agregados exibe uma visão geral dos eventos de desempenho, dados e informações de configuração para cada agregado monitorado por uma instância do Unified Manager. Esta página permite monitorar o desempenho dos seus agregados e solucionar problemas de desempenho e eventos de limite.

A seguir estão alguns campos importantes na visualização Desempenho: Todos os agregados.

- Tipo: O tipo de agregado:

- HDD
 - Híbrido. Combina HDDs e SSDs, mas o Flash Pool não foi habilitado.
 - Híbrido (Flash Pool). Combina HDDs e SSDs, e o Flash Pool foi habilitado.
 - SSD
 - SSD (FabricPool). Combina SSDs e uma camada de nuvem
 - HDD (FabricPool). Combina HDDs e uma camada de nuvem
 - Disco VM (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 o recurso de relatório de dados inativos está habilitado ou desabilitado neste agregado. Quando ativados, os volumes neste 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 oferece suporte a relatórios de dados inativos.
 - Política de limite: a política ou políticas de limite de desempenho definidas pelo usuário que estão ativas neste objeto de armazenamento. Você pode posicionar o cursor sobre os nomes de políticas que contêm reticências (...) para visualizar o nome completo da política ou a lista de nomes de políticas atribuídos. Os botões Atribuir política de limite de desempenho e Limpar política de limite de desempenho permanecem desabilitados até que você selecione um ou mais objetos clicando nas caixas de seleção localizadas na extrema esquerda. Veja os links a seguir para mais informações:
 - ["Atribuindo políticas de limite de desempenho a objetos de armazenamento"](#)
 - ["Removendo políticas de limite de desempenho de objetos de armazenamento"](#)

Desempenho: visualização de todos os nós

A exibição Desempenho: Todos os nós exibe uma visão geral dos eventos de desempenho, dados e informações de configuração para cada nó que está sendo monitorado por uma instância do Unified Manager. Isso permite que você monitore rapidamente o desempenho dos seus nós e solucione problemas de desempenho e eventos de limite.



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 está instalado no nó.

No menu **Relatórios**, a opção **Relatório de inventário de hardware** é fornecida quando o Unified Manager e os clusters que ele gerencia são instalados em um site sem conectividade de rede externa. Este botão gera um arquivo .csv que contém uma lista completa de informações do cluster e do nó; como números de modelo de hardware e números de série, tipos e contagens de disco, licenças instaladas e muito mais. Essa funcionalidade de relatório é útil para renovação de contratos em sites seguros que não estão conectados à plataforma NetApp Active IQ. Você pode atribuir ou limpar políticas de limite de desempenho 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**.

Veja os links a seguir para mais informações:

- ["Atribuindo políticas de limite de desempenho a objetos de armazenamento"](#)
- ["Removendo políticas de limite de desempenho de objetos de armazenamento"](#)
- ["Gerando um relatório de inventário de hardware para renovação de contrato"](#)

Desempenho: visualização de todas as VMs de armazenamento

A exibição Desempenho: todas as VMs de armazenamento exibe uma visão geral dos eventos de desempenho, dados e informações de configuração para cada máquina virtual de armazenamento (SVM) que está sendo monitorada por uma instância do Unified Manager. Isso permite que você monitore rapidamente o desempenho de suas SVMs e solucione problemas de desempenho e eventos de limite. O campo Latência nesta página informa o tempo médio de resposta para todas as solicitações de E/S, expresso em milissegundos por operação.



Os SVMs listados nesta página incluem apenas SVMs de dados e cluster. O Unified Manager não usa nem exibe SVMs de administrador ou de nó.

Veja os links a seguir para mais informações:

- ["Atribuindo políticas de limite de desempenho a objetos de armazenamento"](#)
- ["Removendo políticas de limite de desempenho de objetos de armazenamento"](#)

Desempenho: visualização de todos os LUNs

A exibição Desempenho: Todos os LUNs exibe uma visão geral dos eventos de desempenho, dados e informações de configuração para cada LUN que está sendo monitorado por uma instância do Unified Manager. Isso permite que você monitore rapidamente o desempenho dos seus LUNs e solucione problemas de desempenho e eventos de limite.

Se você quiser analisar a latência e a taxa de transferência de um objeto específico, clique no ícone mais  , então **Analisar carga de trabalho** e você poderá visualizar gráficos de desempenho e capacidade na página **Análise de carga de trabalho**.

Veja os links a seguir para mais informações:

- ["Monitoramento de LUNs em um relacionamento de grupo de consistência"](#)
- ["Provisionamento de LUNs"](#)
- ["Atribuindo políticas de limite de desempenho a objetos de armazenamento"](#)
- ["Removendo políticas de limite de desempenho de objetos de armazenamento"](#)
- ["Exibindo volumes ou LUNs que estão no mesmo grupo de política de QoS"](#)
- ["Visualizando as configurações do grupo de políticas de QoS aplicadas a volumes ou LUNs específicos"](#)
- ["Provisionamento de LUNs usando APIs"](#)

Desempenho: Visualização de todos os namespaces NVMe

A exibição Desempenho: Todos os namespaces NVMe exibe uma visão geral dos eventos de desempenho, dados e informações de configuração para cada namespace NVMe que está sendo monitorado por uma instância do Unified Manager. Isso permite que você monitore rapidamente o desempenho e a integridade dos seus 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 na NVRAM. * Erro de espaço - O namespace ficou sem espaço.

Veja os links a seguir para mais informações:

- ["Atribuindo políticas de limite de desempenho a objetos de armazenamento"](#)
- ["Removendo políticas de limite de desempenho de objetos de armazenamento"](#)

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 esta 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:** Operações de entrada/saída por segundo. O IOPS não é aplicável a NFS LIFs e CIFS LIFs e é exibido como N/A para esses tipos.
- **Latência:** Tempo médio de resposta para todas as solicitações de E/S, expresso em milissegundos por operação. A latência não é aplicável a NFS LIFs e CIFS LIFs e é exibida como N/A para esses tipos.
- **Localização inicial:** a localização inicial da interface, exibida como nome do nó e nome da porta, separados por dois pontos (:). Se o local for exibido com reticências (...), você pode posicionar o cursor sobre o nome do local para visualizar o local completo.
- **Localização atual:** a localização atual da interface, exibida como nome do nó e nome da porta, separados por dois pontos (:). Se o local for exibido com reticências (...), você pode posicionar o cursor sobre o nome do local para visualizar o local completo.
- **Função:** A função da interface: Dados, Cluster, Gerenciamento de Nós ou Intercluster.



As interfaces listadas nesta página incluem LIFs de dados, LIFs de cluster, LIFs de gerenciamento de nós e LIFs intercluster. O Unified Manager não usa nem exibe LIFs do sistema.

Desempenho: Visualização de todas as portas

A exibição Desempenho: Todas as portas exibe uma visão geral dos eventos de desempenho, dados e informações de configuração para 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 da porta de rede é exibida, 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 somente para portas físicas. Os valores do contador não são exibidos para VLANs ou grupos de interface.

Veja os links a seguir para mais informações:

- ["Atribuindo políticas de limite de desempenho a objetos de armazenamento"](#)
- ["Removendo políticas de limite de desempenho de objetos de armazenamento"](#)

Desempenho: visualização de grupos de políticas de QoS

A exibição Grupos de políticas de QoS exibe os grupos de políticas de QoS disponíveis nos clusters que o Unified Manager está monitorando. Isso inclui políticas de QoS tradicionais, políticas de QoS adaptáveis e políticas de QoS atribuídas usando Níveis de Serviço de Desempenho.

A seguir estão alguns campos importantes na exibição Desempenho: Grupos de políticas de QoS.

- Grupo de política de QoS: o nome do grupo de política de QoS. Para políticas do NetApp Service Level Manager (NSLM) 1.3 que foram importadas para o Unified Manager 9.7 ou superior, o nome exibido aqui inclui o nome do SVM e outras informações que não estão no nome quando o Performance Service Level foi definido no NSLM. Por exemplo, o nome "NSLM_vs6_Performance_2_0" significa que esta é a política PSL de "Desempenho" definida pelo sistema NSLM, criada no SVM "vs6" com uma latência esperada de "2 ms/op".
- SVM: A VM de armazenamento (SVM) à qual o grupo de política de QoS pertence. Você pode clicar no nome da VM de armazenamento para navegar até a página de detalhes dessa VM de armazenamento. Observe que este campo estará em branco se a política de QoS tiver sido criada na VM de armazenamento do administrador, pois esse tipo de VM de armazenamento representa o cluster.
- Taxa de transferência mínima: a taxa de transferência mínima, em IOPS, que o grupo de políticas terá a garantia de fornecer. Para políticas adaptáveis, esse é o IOPS mínimo esperado por TB alocado ao volume ou LUN, com base no tamanho alocado do objeto de armazenamento.
- 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 estiver em branco, significa que o máximo definido no ONTAP é infinito. Para políticas adaptáveis, esse é o IOPS máximo (pico) 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 adaptativas, este é o valor mínimo absoluto de IOPS que é 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 IOPS de taxa de transferência máxima (pico).
- Latência esperada: a latência média esperada para operações de entrada/saída de armazenamento.
- 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 ver 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 no momento.
- Objetos associados: o número de cargas de trabalho atribuídas ao grupo de políticas de QoS, separadas em volumes e LUNs. Você pode clicar no número para navegar até uma página que fornece mais detalhes sobre os volumes ou LUNs selecionados.

Para mais informações, consulte os tópicos em ["Gerenciando o desempenho usando informações do grupo de políticas de QoS"](#).

Refinando o conteúdo da página de inventário de desempenho

As páginas de inventário para objetos de desempenho contêm ferramentas para ajudar você a refinar o conteúdo de dados de inventário de objetos, permitindo que você localize dados específicos de forma rápida e fácil.

As informações contidas nas páginas de inventário de objetos de desempenho podem ser extensas, muitas vezes abrangendo várias páginas. Esse tipo de dado abrangente é excelente para monitorar, rastrear e melhorar o desempenho; no entanto, localizar dados específicos requer ferramentas que permitam localizar rapidamente os dados que você está procurando. Portanto, as páginas de inventário de objetos de

desempenho contêm funcionalidades para pesquisa, classificação e filtragem. Além disso, a pesquisa e a filtragem podem funcionar juntas para refinar ainda mais seus resultados.

Pesquisar nas páginas de desempenho do inventário de objetos

Você pode pesquisar strings nas páginas de Desempenho do Inventário de Objetos. Use o campo **Pesquisar** localizado no canto superior direito da página para localizar rapidamente dados com base no nome do objeto ou no nome da política. Isso permite que você localize rapidamente objetos específicos e seus dados associados, ou localize rapidamente políticas e visualize dados de objetos de políticas associados.

Etapa

1. Execute uma das seguintes opções, com base nos seus requisitos de pesquisa:

Para localizar isto...	Digite isto...
Um objeto específico	Digite o nome do objeto no campo Pesquisar e clique em Pesquisar . O objeto que você pesquisou e seus dados relacionados são exibidos.
Uma política de limite de desempenho definida pelo usuário	Digite todo ou parte do nome da política no campo Pesquisar e clique em Pesquisar . Os objetos atribuídos à política que você pesquisou são exibidos.

Classificar nas páginas de desempenho do inventário de objetos

Você pode classificar todos os dados nas páginas de Desempenho do Inventário de Objetos por qualquer coluna em ordem crescente ou decrescente. Isso permite que você localize 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 título de coluna destacado e um ícone de seta indicando a direção da classificação à direita do nome. Uma seta para cima indica ordem crescente; uma seta para baixo indica ordem decrescente. A ordem de classificação padrão é por **Status** (criticidade do evento) em ordem decrescente, com os eventos de desempenho mais críticos listados primeiro.

Etapa

1. Você pode clicar no nome de uma coluna para alternar a ordem de classificação da coluna em ordem crescente ou decrescente.

O conteúdo da página Desempenho do inventário de objetos é classificado em ordem crescente ou decrescente, com base na coluna selecionada.

Filtrar dados nas páginas de desempenho do inventário de objetos

Você pode filtrar dados nas páginas Desempenho do inventário de objetos para localizar dados rapidamente com base em critérios específicos. Você pode usar a filtragem para restringir o conteúdo das páginas de Desempenho do Inventário de Objetos para mostrar

apenas os resultados especificados. Isso fornece um método muito eficiente de exibir apenas os dados de desempenho nos quais você está interessado.

Você pode usar o painel Filtragem para personalizar a visualização em grade com base em suas preferências. As opções de filtro disponíveis são baseadas no tipo de objeto visualizado na grade. Se filtros estiverem aplicados no momento, o número de filtros aplicados será exibido à direita do botão Filtro.

Três tipos de parâmetros de filtro são suportados.

Parâmetro	Validação
String (texto)	Os operadores são contém , começa com , termina com e não contém .
Número	Os operadores são maior que , menor que , no último e entre .
Enum (texto)	Os operadores são is e is not .

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 quatro. Os resultados filtrados são baseados em parâmetros de filtro combinados. Os resultados filtrados se aplicam a todas as páginas da sua pesquisa filtrada, não apenas à página exibida no momento.

Você pode adicionar filtros usando o painel Filtragem.

1. No topo da página, clique no botão **Filtro**. O painel Filtragem é exibido.
2. Clique na lista suspensa à esquerda e selecione um objeto; por exemplo, *Cluster* ou um contador de desempenho.
3. Clique na lista suspensa central e selecione o operador que deseja usar.
4. Na última lista, selecione ou insira um valor para completar o filtro para aquele objeto.
5. Para adicionar outro filtro, clique em **+Adicionar filtro**. Um campo de filtro adicional é exibido. Complete este filtro usando o processo descrito nas etapas anteriores. Observe que ao adicionar seu quarto filtro, o botão **+Adicionar Filtro** não será mais exibido.
6. Clique em **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 **Redefinir** 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				
				Cancel Apply Filter

Após clicar em **Aplicar filtro**, o painel Filtragem fecha, aplica seus filtros e mostra o número de filtros aplicados (3).

Entenda as recomendações do Unified Manager para hierarquizar dados na nuvem

A exibição Desempenho: Todos os volumes exibe informações relacionadas ao tamanho dos dados do usuário armazenados no volume que está inativo (frio). Em alguns casos, o Unified Manager identifica determinados volumes que se beneficiariam da hierarquização dos dados inativos na camada de nuvem (provedor 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 à 9.2, a recomendação do Unified Manager para hierarquizar dados exige a atualização do seu software ONTAP . Além disso, o **auto** A política de hierarquização foi introduzida no ONTAP 9.4 e a **all** A política de hierarquização foi introduzida no ONTAP 9.6, portanto, se a recomendação for usar a política de hierarquização automática, você deve atualizar para o ONTAP 9.4 ou superior.

Os três campos a seguir na exibição Desempenho: Todos os volumes fornecem informações sobre se você pode melhorar a utilização do disco do seu sistema de armazenamento e economizar espaço na camada de desempenho movendo dados inativos para a camada de nuvem.

• Política de níveis

A política de camadas determina se os dados no volume permanecem na camada de desempenho ou se alguns dos dados são movidos da camada de desempenho para a camada de nuvem.

O valor neste campo indica a política de camadas definida no volume, mesmo que o volume não resida atualmente em um agregado FabricPool . A política de hierarquização entra em vigor somente quando o volume está em um agregado FabricPool .

• Dados Frios

Os dados frios exibem o tamanho dos dados do usuário armazenados no volume que está inativo (frio).

Um valor é exibido aqui somente ao usar o software ONTAP 9.4 ou superior porque ele requer que o agregado no qual o volume é implantado tenha o **inactive data reporting parameter** definido para **enabled** , e que o limite mínimo de dias de resfriamento foi atingido (para volumes que utilizam o **snapshot-only** ou **auto** política de hierarquização). Caso contrário, o valor será listado como "N/A".

• Recomendação de Nuvem

Depois que informações suficientes forem capturadas sobre a atividade de dados no volume, o Unified Manager poderá determinar que nenhuma ação é necessária ou que você pode economizar espaço na camada de desempenho hierarquizando dados inativos na camada de nuvem.



O campo Dados frios é atualizado a cada 15 minutos, mas o campo Recomendação de nuvem é atualizado a cada 7 dias quando a análise de dados frios é realizada no volume. Portanto, a quantidade exata de dados frios pode diferir entre os campos. O campo Recomendação de Nuvem exibe a data em que a análise foi executada.

Quando o Relatório de Dados Inativos está ativado, o campo Dados Frios exibe a quantidade exata de dados inativos. Sem o recurso de relatório de dados inativos, o Unified Manager usa estatísticas de desempenho para determinar se os dados estão inativos em um volume. A quantidade de dados inativos não é exibida no campo Dados Frios neste caso, mas é exibida quando você passa o cursor sobre a palavra **Nível** para visualizar a recomendação da nuvem.

As recomendações de nuvem que você verá são:

- **Aprendizado.** 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 mover esses dados 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 camadas.
- **Nenhuma ação.** O volume tem muito poucos dados inativos, o volume já está definido para a política de hierarquização “auto” em um agregado FabricPool ou o volume é um volume de proteção de dados. Este valor também é exibido quando o volume está offline ou quando está sendo usado em uma configuração do MetroCluster.

Para mover um volume ou alterar a política de camadas de volume ou as configurações de relatórios de dados inativos agregados, use o ONTAP System Manager, os comandos ONTAP CLI ou uma combinação dessas ferramentas.

Se você estiver conectado ao Unified Manager com a função de 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 Gerenciador do Sistema para fazer a alteração recomendada.

Monitore o 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 do 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 dos objetos em um formato lado a lado.

Entenda o objeto raiz

O objeto raiz é a linha de base com a qual outras comparações de objetos são feitas. Isso permite que você visualize e compare os dados de outros objetos com o objeto raiz, fornecendo análise de dados de desempenho que ajuda a solucionar problemas e melhorar o desempenho do objeto.

O nome do objeto raiz é exibido na parte superior do painel 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 Comparação, somente um objeto raiz é permitido. Os dados do objeto raiz são exibidos automaticamente nos gráficos no painel Gráficos do Contador.

Não é possível alterar o objeto raiz; ele é sempre definido como a página do objeto que você está visualizando. Por exemplo, se você abrir a página Volume Performance Explorer do Volume1, o Volume1 será o objeto raiz e não poderá ser alterado. Se quiser comparar com um objeto raiz diferente, você deve clicar no link de um objeto e abrir sua página de destino.



Eventos e Limites são exibidos somente para objetos raiz.

Aplique filtragem para reduzir a lista de objetos correlacionados na grade

A filtragem permite que você exiba um subconjunto menor e mais bem definido de objetos na grade. Por exemplo, se você tiver 25 volumes na grade, a filtragem permitirá que você visualize apenas os volumes com taxa de transferência menor que 90 MBps ou latência maior que 1 ms/op.

Especifique um intervalo de tempo para objetos correlacionados

O seletor de intervalo de tempo na página Performance Explorer permite que você especifique o intervalo de tempo para comparação de dados de 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 nos quais você está interessado. Você pode selecionar um intervalo de tempo predefinido ou especificar um intervalo de tempo personalizado. O intervalo de tempo padrão são as 72 horas anteriores.

Selecione um intervalo de tempo predefinido

Selecionar um intervalo de tempo predefinido é uma maneira 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, dados de até 13 meses estarão disponíveis.

Passos

1. No canto superior direito da página **Performance Explorer**, clique em **Intervalo de tempo**.
2. No lado direito do painel **Seleção de intervalo de tempo**, selecione um intervalo de tempo predefinido.
3. Clique em **Aplicar intervalo**.

Especifique um intervalo de tempo personalizado

A página Performance Explorer permite que você especifique o intervalo de data e hora para seus dados de desempenho. Especificar um intervalo de tempo personalizado oferece maior flexibilidade do que usar intervalos de tempo predefinidos ao refinar dados de objetos de cluster.

Você pode selecionar um intervalo de tempo entre uma hora e 390 dias. 13 meses equivalem 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 ajuda a solucionar possíveis problemas de desempenho, pois especificar um intervalo de data e hora exibe dados sobre o evento de desempenho com mais detalhes. 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 **Última hora** até **Últimos 13 meses**.

Selecionar a opção **Últimos 13 meses** ou especificar um intervalo de datas personalizado maior que 30 dias exibe uma caixa de diálogo alertando que os dados de desempenho exibidos para um período maior que 30 dias são mapeados usando médias horárias e não pesquisas de dados de 5 minutos. Portanto, pode ocorrer uma perda de granularidade visual da linha do tempo. Se você clicar na opção **Não mostrar novamente** na caixa de diálogo, a mensagem não aparecerá quando você selecionar a opção **Últimos 13 meses** ou especificar um intervalo de datas personalizado maior que 30 dias. Os dados resumidos também se aplicam a um intervalo de tempo menor, se o intervalo de tempo incluir uma hora/data superior a 30 dias a partir de hoje.

Ao selecionar um intervalo de tempo (personalizado ou predefinido), intervalos de tempo de 30 dias ou menos são baseados em amostras de dados de intervalo de 5 minutos. Intervalos de tempo maiores que 30 dias são baseados em amostras de dados de intervalo de uma hora.

The screenshot shows the 'Intervalo de tempo' (Time Range) dialog box. It features two calendar views, 'From' and 'To', both for April 2015. The 'From' calendar has the 12th selected, and the 'To' calendar has the 15th selected. Below the calendars are time selectors for 'From' and 'To', both set to '6:00 am'. To the right of the calendars is a list of predefined time ranges: 'Last Hour', 'Last 24 Hours', 'Last 72 Hours', 'Last 7 Days', 'Last 30 Days', 'Last 13 Months', and 'Custom Range'. The 'Custom Range' option is currently selected. At the bottom right are 'Cancel' and 'Apply Range' buttons.

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 em um dos botões **Último...** à direita do painel **Intervalo de tempo**. Ao selecionar um intervalo de tempo predefinido, dados de até 13 meses estarão disponíveis. O botão de intervalo de tempo predefinido que você selecionou é destacado, e os dias e horários correspondentes são exibidos nos calendários e seletores de horário.
3. Para selecionar um intervalo de datas personalizado, clique na data de início no calendário **De** à esquerda. Clique em **<** ou **>** para navegar para frente ou para trás no calendário. Para especificar a data final, clique em uma data no calendário **Até** à direita. Observe que a data final padrão é hoje, a menos que você especifique uma data final diferente. O botão **Intervalo personalizado** à direita do painel Intervalo de tempo é destacado, indicando que você selecionou um intervalo de datas personalizado.

4. Para selecionar um intervalo de tempo personalizado, clique no controle **Tempo** abaixo do calendário **De** e selecione a hora de início. Para especificar o horário de término, clique no controle **Hora** abaixo do calendário **Até** à direita e selecione o horário de término. O botão **Intervalo personalizado** à direita do painel Intervalo de tempo é destacado, indicando que você 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 depois selecione os horários de início e término, conforme descrito anteriormente. As datas selecionadas são destacadas nos calendários, os horários de início e término especificados são exibidos nos controles **Tempo** e o botão **Intervalo personalizado** é destacado.
6. Após 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.

Defina 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 Gráfico de Contadores. Por exemplo, se sua máquina virtual de armazenamento (SVM) estiver apresentando problemas de desempenho, você poderá comparar todos os volumes na SVM para identificar qual volume pode estar causando o problema.

Você pode adicionar qualquer objeto na grade de objetos correlacionados aos painéis Gráfico de 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 da grade de objetos correlacionados; no entanto, o objeto raiz no painel Comparação não pode ser removido.



Adicionar muitos objetos ao painel 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 de objetos, localize o objeto que você deseja adicionar e clique no botão **Adicionar**.

O botão **Adicionar** fica cinza e o objeto é adicionado à lista de objetos adicionais no painel Comparação. Os dados do objeto são adicionados aos gráficos nos painéis Gráficos do Contador. A cor do ícone do 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 atitude...
Ocultar um objeto selecionado	Clique no ícone do olho do objeto selecionado () no painel Comparação. Os dados do objeto ficam ocultos e o ícone de olho desse objeto fica cinza.

Para fazer isso...	Tome esta atitude...
Mostrar um objeto oculto	Clique no ícone de olho cinza do objeto selecionado no painel Comparação. O ícone do olho retorna à sua cor original e os dados do objeto são adicionados novamente aos gráficos no painel Gráficos do Contador.

3. **Opcional:** Remova os objetos selecionados do painel **Comparando**:

Para fazer isso...	Tome esta atitude...
Remover um objeto selecionado	Passe o mouse sobre o nome do objeto selecionado no painel Comparação para mostrar o botão remover objeto (X) e, em seguida, clique no botão. O objeto é removido do painel Comparação e seus dados são limpos dos gráficos de contagem.
Remover todos os objetos selecionados	Clique no botão remover todos os objetos (X) na parte superior do painel Comparação. Todos os objetos selecionados e seus dados são removidos, deixando apenas o objeto raiz.

Entenda os gráficos de contador

Os gráficos no painel Gráficos do contador permitem que você visualize e compare dados de desempenho do objeto raiz e dos objetos que você adicionou da grade de objetos correlacionados. Isso pode ajudar você a entender tendências de desempenho e isolar e resolver problemas de desempenho.

Os gráficos de contadores exibidos por padrão são Eventos, Latência, IOPS e MBps. Os gráficos opcionais que você pode escolher exibir são Utilização, Capacidade de desempenho usada, IOPS disponíveis, IOPS/TB e Taxa de falhas de cache. Além disso, você pode optar por visualizar valores totais ou detalhados para os gráficos de Latência, IOPS, MBps e Capacidade de Desempenho Utilizada.

O Performance Explorer exibe determinados gráficos de contadores por padrão, independentemente de o objeto de armazenamento oferecer suporte a todos eles ou não. Quando um contador não é suportado, o gráfico do contador fica vazio e a mensagem `Not applicable for <object>` é exibido.

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**

Exibe o período de tempo especificado. Se você não especificou um intervalo de tempo, o padrão é o período anterior de 72 horas.

- **Eixo Y**

Exibe unidades de contagem exclusivas para o objeto ou objetos selecionados.

As cores das linhas de tendência correspondem à cor do nome do objeto, conforme exibido no painel 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 em um gráfico, poderá usar um dos seguintes métodos:

- Use o botão < para expandir o painel Gráficos de Contagem para abranger a largura da página.
- Use o cursor (quando ele se transformar em uma lupa) para selecionar uma parte do período no gráfico para focar e ampliar essa área. Você pode clicar em Redefinir zoom do gráfico para retornar o gráfico ao período padrão.
- Use o botão **Visualização de Zoom** para exibir um gráfico grande de contador único que contém detalhes expandidos e indicadores de limite.



Ocasionalmente, lacunas nas linhas de tendência são exibidas. Lacunas significam que o Unified Manager falhou ao coletar dados de desempenho do sistema de armazenamento 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 detalhamento exibe os valores totais separados em leitura, gravação e outras categorias. Além disso, alguns gráficos de contador de detalhamento exibem detalhes adicionais quando o gráfico é exibido na visualização Zoom.

A tabela a seguir mostra os gráficos de contadores de desempenho disponíveis.

Gráficos disponíveis	Descrição do gráfico
Eventos	Exibe eventos críticos, de erro, de aviso e de informação em correlação com os gráficos estatísticos do objeto raiz. Os eventos de saúde são exibidos além dos eventos de desempenho para fornecer uma imagem 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 - Análise	As mesmas informações mostradas em Latência Total, mas com os dados de desempenho separados em leitura, gravação e outras latências. Esta opção de gráfico se aplica somente quando o objeto selecionado é um SVM, nó, agregado, volume, LUN ou namespace.

Gráficos disponíveis	Descrição do gráfico
Latência - Componentes do Cluster	As mesmas informações mostradas em Latência Total, mas com os dados de desempenho separados em latência por componente do cluster. Esta opção de gráfico se aplica somente 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 por esse nó e que podem residir no nó local ou remoto, e selecionar “Total (Local)” exibe o IOPS para dados que residem somente no nó atual.
IOPS - Análise	As mesmas informações mostradas no Total de IOPS, mas com os dados de desempenho separados em leitura, gravação e outros IOPS. Esta opção de gráfico se aplica somente quando o objeto selecionado é um SVM, nó, agregado, volume, LUN ou namespace. Quando exibido na visualização Zoom, o gráfico de volumes exibe valores mínimos e máximos de taxa de transferência de QoS, se configurado no ONTAP. Quando exibido para um nó, selecionar “Breakdown” exibe o detalhamento de IOPS para dados que se movem por esse nó e que podem residir no nó local ou remoto, e selecionar “Breakdown (Local)” exibe o detalhamento de IOPS para dados que residem somente no nó atual.
IOPS - Protocolos	As mesmas informações mostradas no IOPS Total, mas os dados de desempenho são separados em gráficos individuais para tráfego de protocolo CIFS, NFS, FCP, NVMe e iSCSI. Esta opção de gráfico se aplica somente quando o objeto selecionado é um SVM.

Gráficos disponíveis	Descrição do gráfico
IOPS/TB - Total	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, esse contador mede quanto desempenho pode ser fornecido por uma determinada quantidade de capacidade de armazenamento. Quando exibido na visualização Zoom, o gráfico de volumes exibe os valores de QoS esperados e de pico de taxa de transferência, se configurado no ONTAP. Esta opção de gráfico se aplica somente quando o objeto selecionado é um volume.
MB/s - Total	Número de megabytes de dados transferidos de e para o objeto por segundo.
MB/s - Repartição	As mesmas informações mostradas no gráfico MB/s, mas com os dados de taxa de transferência separados em leituras de disco, leituras de Flash Cache, gravações e outros. Quando exibido na visualização Zoom, o gráfico de volumes exibe valores máximos de taxa de transferência de QoS, se configurado no ONTAP. Esta opção de gráfico se aplica somente quando o objeto selecionado é um SVM, nó, agregado, volume, LUN ou namespace.  Os dados do Flash Cache são exibidos somente para nós e somente quando um módulo Flash Cache está instalado no nó.
Capacidade de Desempenho Utilizada - Total	Porcentagem da capacidade de desempenho que está sendo consumida pelo nó ou agregado.
Capacidade de Desempenho Utilizada - Detalhamento	Capacidade de desempenho Dados usados separados em protocolos de usuário e processos em segundo plano do sistema. Além disso, a quantidade de capacidade de desempenho livre é mostrada.
IOPS disponíveis - Total	Número de operações de entrada/saída por segundo que estão atualmente disponíveis (gratuitas) neste objeto. Esse número é o resultado da subtração do IOPS usado atualmente do IOPS total que o Unified Manager calcula que o objeto pode executar. Esta opção de gráfico se aplica somente quando o objeto selecionado é um nó ou agregado.

Gráficos disponíveis	Descrição do gráfico
Utilização - Total	Porcentagem de recursos disponíveis do objeto que está sendo usado. A utilização indica a utilização do nó para nós, a utilização do disco para agregados e a utilização da largura de banda para portas. Esta 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 se aplica somente quando o objeto selecionado é um volume.

Selecione gráficos de desempenho para exibir

A lista suspensa Escolher gráficos permite que você selecione os tipos de gráficos de contadores de desempenho a serem exibidos no painel Gráficos de contadores. Isso permite que você visualize dados e contadores específicos, com base em seus requisitos de desempenho.

Passos

1. No painel **Gráficos do contador**, clique na lista suspensa **Escolher gráficos**.
2. Adicionar ou remover gráficos:

Para...	Faça isso...
Adicionar ou remover gráficos individuais	Clique nas caixas de seleção ao lado dos gráficos que você deseja mostrar ou ocultar
Adicionar todos os gráficos	Clique em Selecionar tudo
Remover todos os gráficos	Clique em Desmarcar tudo

Suas seleções de gráficos são exibidas no painel Gráficos de Contadores. Observe que, à medida que você adiciona gráficos, os novos gráficos são inseridos no painel Gráficos do contador para corresponder à ordem dos gráficos listados na lista suspensa Escolher gráficos. Selecionar gráficos adicionais pode exigir rolagem adicional.

Expandir o painel Gráficos de Contadores

Você pode expandir o painel Gráficos de Contadores para que os gráficos fiquem maiores e mais legíveis.

Depois de definir os objetos de comparação e o intervalo de tempo para os contadores, você pode visualizar um painel maior de Gráficos de Contadores. Use o botão < no meio da janela do Performance Explorer para expandir o painel.

Etapa

1. Expanda ou reduza o painel **Gráficos de Contadores**.

Para...	Faça isso...
Expanda o painel Gráficos de Contagem para ajustar a largura da página	Clique no botão <
Reduza o painel Gráficos de Contagem para a metade direita da página	Clique no botão *>

Alterar o foco dos gráficos de contador para um período de tempo mais curto

Você pode usar o mouse para reduzir o intervalo de tempo e focar em um período específico no painel Gráfico do Contador ou na janela Exibição de Zoom dos Gráficos do Contador. Isso permite que você tenha uma visão mais granular e microscópica de qualquer parte da linha do tempo de dados de desempenho, eventos e limites.

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 tempo e data no seletor **Intervalo de tempo** não muda dos valores originais do gráfico.

Passos

1. Para ampliar um período específico de tempo, clique usando a lupa e arraste o mouse para destacar a área que você deseja ver em detalhes.

Os valores do contador para o período de tempo selecionado preenchem o gráfico do contador.

2. Para retornar ao período de tempo original definido no seletor **Intervalo de tempo**, clique no botão **Redefinir zoom do gráfico**.

O gráfico do contador é exibido em seu estado original.

Ver detalhes do evento na Linha do tempo de eventos

Você pode visualizar 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 na solução de problemas de desempenho.

O painel Linha do tempo 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 seu próprio cronograma. 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 distribui vários eventos

em eventos únicos, permitindo que você visualize e investigue cada evento separadamente.

Cada ponto de evento de desempenho na Linha do tempo de eventos se alinha verticalmente com um pico correspondente nas linhas de tendência dos gráficos de contagem que são exibidas abaixo da Linha do tempo de eventos. Isso fornece uma correlação visual direta entre eventos e desempenho geral. Os eventos de saúde também são exibidos na linha do tempo, mas esses tipos de eventos não necessariamente correspondem a um pico em um dos gráficos de desempenho.

Passos

- 1. No painel **Linha do tempo de eventos**, posicione o cursor sobre um ponto de evento em uma linha do tempo para visualizar um resumo do evento ou eventos naquele ponto do 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 detalhes completos do evento para um evento ou vários eventos:

Para fazer isso...	Clique aqui...
Ver detalhes de um único evento	Ver detalhes do evento na caixa de diálogo pop-up.
Ver detalhes de vários eventos	Ver detalhes do evento na caixa de diálogo pop-up.  Clicar em um único evento na caixa de diálogo de vários eventos exibe a página Detalhes do evento apropriada.

Visualização de zoom de gráficos de contador

Os gráficos de contador fornecem uma visualização de zoom que permite que você amplie os detalhes de desempenho ao longo do período de tempo especificado. Isso permite que você veja detalhes de desempenho e eventos com granularidade muito maior, o que é benéfico ao solucionar problemas de desempenho.

Quando exibidos na Visualização de Zoom, alguns gráficos de detalhamento fornecem informações adicionais do que aquelas que aparecem quando o gráfico não está na Visualização de Zoom. Por exemplo, as páginas de exibição de zoom do gráfico de detalhamento de IOPS, IOPS/TB e MBps exibem valores de política de QoS para volumes e LUNs, se eles tiverem sido definidos no ONTAP.



Para políticas de limite de desempenho definidas pelo sistema, somente as políticas “Recursos do nó superutilizados” 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.

Exibir a visualização de zoom dos gráficos do contador

A visualização de zoom dos 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.

Você pode exibir a Visualização de Zoom dos Gráficos de Contadores para qualquer gráfico de contadores.

Passos

1. Clique em **Visualização com Zoom** para abrir o gráfico selecionado em uma nova janela do navegador.
2. Se você estiver visualizando um gráfico de detalhamento e clicar em **Visualização com zoom**, o gráfico de detalhamento será exibido na Visualização com zoom. Você pode selecionar **Total** enquanto estiver na Visualização de Zoom se quiser alterar a opção de visualização.

Especifique o intervalo de tempo na visualização do Zoom

O controle **Intervalo de tempo** na janela Exibição de zoom de gráficos de contador permite que você especifique um intervalo de data e hora para o gráfico selecionado. Isso permite que você localize rapidamente dados específicos com base em um intervalo de tempo predefinido ou em seu próprio intervalo de tempo personalizado.

Você pode selecionar um intervalo de tempo entre uma hora e 390 dias. 13 meses equivalem 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 ajuda a solucionar possíveis problemas de desempenho, pois especificar um intervalo de data e hora exibe dados sobre o evento de desempenho com mais detalhes. 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 **Última hora** até **Últimos 13 meses**.

Selecionar a opção **Últimos 13 meses** ou especificar um intervalo de datas personalizado maior que 30 dias exibe uma caixa de diálogo alertando que os dados de desempenho exibidos para um período maior que 30 dias são mapeados usando médias horárias e não pesquisas de dados de 5 minutos. Portanto, pode ocorrer uma perda de granularidade visual da linha do tempo. Se você clicar na opção **Não mostrar novamente** na caixa de diálogo, a mensagem não aparecerá quando você selecionar a opção **Últimos 13 meses** ou especificar um intervalo de datas personalizado maior que 30 dias. Os dados resumidos também se aplicam a um intervalo de tempo menor, se o intervalo de tempo incluir uma hora/data superior a 30 dias a partir de hoje.

Ao selecionar um intervalo de tempo (personalizado ou predefinido), intervalos de tempo de 30 dias ou menos são baseados em amostras de dados de intervalo de 5 minutos. Intervalos de tempo maiores que 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 em um dos botões **Último...** à direita do painel **Intervalo de tempo**. Ao selecionar um intervalo de tempo predefinido, dados de até 13 meses estarão disponíveis. O botão de intervalo de tempo predefinido que você selecionou é destacado, e os dias e horários correspondentes são exibidos nos calendários e seletores de horário.
3. Para selecionar um intervalo de datas personalizado, clique na data de início no calendário **De** à esquerda. Clique em **<** ou **>** para navegar para frente ou para trás no calendário. Para especificar a data final, clique em uma data no calendário **Até** à direita. Observe que a data final padrão é hoje, a menos que você especifique uma data final diferente. O botão **Intervalo personalizado** à direita do painel Intervalo de tempo é destacado, indicando que você selecionou um intervalo de datas personalizado.
4. Para selecionar um intervalo de tempo personalizado, clique no controle **Tempo** abaixo do calendário **De** e selecione a hora de início. Para especificar o horário de término, clique no controle **Hora** abaixo do calendário **Até** à direita e selecione o horário de término. O botão **Intervalo personalizado** à direita do painel Intervalo de tempo é destacado, indicando que você 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 depois selecione os horários de início e término, conforme descrito anteriormente. As datas selecionadas são destacadas nos calendários, os horários de início e término especificados são exibidos nos controles **Tempo** e o botão **Intervalo personalizado** é destacado.
6. Após 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.

Selecione limites de desempenho na visualização de zoom dos gráficos do contador

A aplicação de limites na Exibição de zoom dos gráficos de contadores fornece uma visão detalhada das ocorrências de eventos de limite de desempenho. Isso permite que você aplique ou remova limites e visualize os resultados imediatamente, o que pode ser útil ao decidir se a solução de problemas deve ser seu próximo passo.

Selecionar limites na Exibição de zoom dos gráficos de contador permite que você visualize dados precisos sobre eventos de limite de desempenho. Você pode aplicar qualquer limite que apareça na área **Políticas** da Visualização de Zoom dos Gráficos de Contagem.

Somente uma política por vez pode ser aplicada ao objeto na Exibição de Zoom de Gráficos de Contadores.

Etapa

1. Selecione ou desmarque o  que está associado a uma política.

O limite selecionado é aplicado à Visualização de Zoom dos Gráficos de Contagem. Os limites críticos são exibidos como uma linha vermelha; os limites de alerta são exibidos como uma linha amarela.

Exibir latência de volume por componente do cluster

Você pode visualizar informações detalhadas de latência de um volume usando a página Volume Performance Explorer. O gráfico Latência - Contador total mostra a latência total no volume, e o gráfico Latência - Contador detalhado é útil para determinar o impacto da latência de leitura e gravação no volume.

Além disso, o gráfico Latência - Componentes do 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
- Limite mínimo de QoS
- Processamento de rede
- Interconexão de cluster
- Data Processing
- Operações Agregadas
- Ativação de Volume
- Recursos do MetroCluster
- Latência da Nuvem
- Sincronizar SnapMirror

Passos

1. Na página **Volume Performance Explorer** do volume selecionado, no gráfico Latência, selecione **Componentes do Cluster** no menu suspenso.

O gráfico Latência - Componentes do Cluster é exibido.

2. Para visualizar uma versão maior do gráfico, selecione **Visualização com Zoom**.

O gráfico comparativo dos componentes do cluster é exibido. 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.

Visualizar tráfego SVM IOPS por protocolo

Você pode visualizar informações detalhadas de IOPS para um SVM usando a página Performance/SVM Explorer. O gráfico de contador total de IOPS mostra o uso total de IOPS no SVM, e o gráfico de contador de detalhamento de 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. Os seguintes protocolos estão disponíveis:

- CIFS
- NFS
- FCP
- iSCSI
- NVMe-FC

Passos

1. Na página **Performance/SVM Explorer** do SVM selecionado, no gráfico IOPS, selecione **Protocolos** no menu suspenso.

O gráfico IOPS - Protocolos é exibido.

2. Para visualizar uma versão maior do gráfico, selecione **Visualização com Zoom**.

O gráfico comparativo do protocolo avançado IOPS é exibido. Você 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 do gráfico de qualquer um dos gráficos para ver a janela pop-up.

Visualize gráficos de volume e latência de LUN para verificar a garantia de desempenho

Você pode visualizar os volumes e LUNs que assinou no programa “Garantia de Desempenho” para verificar se a latência não excedeu o nível garantido.

A garantia de desempenho de latência é um valor de milissegundo por operação que não deve ser excedido. Ela se baseia em uma média horária, não no período padrão de coleta de desempenho de cinco minutos.

Passos

1. Na exibição **Desempenho: Todos os volumes** ou **Desempenho: Todos os LUNs**, selecione o volume ou LUN no qual você está interessado.
2. Na página **Performance Explorer** do volume ou LUN selecionado, escolha **Média horária** no seletor **Exibir estatísticas em**.

A linha horizontal no gráfico de Latência mostrará uma linha mais suave à medida que as coletas de cinco minutos forem substituídas pela média horária.

3. Se você tiver outros volumes no mesmo agregado que estejam sob a garantia de desempenho, poderá adicioná-los para visualizar o valor de latência no mesmo gráfico.

Veja o desempenho de todos os clusters do SAN Array

Você pode usar a exibição **Desempenho: Todos os clusters** para exibir o status de desempenho dos seus clusters do All SAN Array.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode visualizar informações gerais para todos os clusters do SAN Array na exibição Desempenho: Todos os clusters e detalhes na página Cluster/Desempenho Explorer.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Clusters**.
2. Certifique-se de que a coluna “Personalidade” seja exibida na exibição **Saúde: Todos os Clusters** ou adicione-a usando o controle **Mostrar / Ocultar**.

Esta coluna exibe “All SAN Array” para seus clusters All SAN Array.

3. Para visualizar informações sobre o desempenho desses clusters, selecione a visualização **Desempenho: Todos os clusters**.

Veja as informações de desempenho do cluster All SAN Array.

4. Para visualizar informações detalhadas sobre o desempenho desses clusters, clique no nome de um cluster All SAN Array.
5. Clique na aba **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 neste 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 maior para identificar quaisquer problemas de configuração.

Exibir IOPS do nó com base em cargas de trabalho que residem apenas no nó local

O gráfico do contador de IOPS do nó pode destacar onde as operações estão passando apenas pelo nó local usando um LIF de rede para executar operações de leitura/gravação em volumes em um nó remoto. Os gráficos IOPS - “Total (Local)” e “Detalhamento (Local)” exibem o IOPS para dados que residem em volumes locais somente no nó atual.

As versões “locais” desses gráficos de contadores são semelhantes aos gráficos de nós para Capacidade de Desempenho e Utilização porque também mostram apenas as estatísticas de dados que residem em volumes locais.

Ao comparar as versões “Locais” desses gráficos de contadores com as versões Totais regulares desses gráficos de contadores, você pode ver se há muito tráfego passando pelo nó local para acessar volumes no nó remoto. Essa situação pode causar problemas de desempenho, possivelmente indicados pela alta utilização do nó, se houver muitas operações passando pelo nó local para atingir um volume em um nó remoto. Nesses casos, talvez você queira 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 conectado.

Passos

1. Na página **Desempenho/Explorador de Nós** do nó selecionado, no gráfico IOPS, selecione **Total** no menu suspenso.

O gráfico IOPS - Total é exibido.

2. Clique em **Visualização com zoom** para exibir uma versão maior do gráfico em uma nova aba do navegador.
3. De volta à página **Desempenho/Explorador de Nós**, no gráfico IOPS, selecione **Total (Local)** no menu suspenso.

O gráfico IOPS - Total (Local) é exibido.

4. Clique em **Visualização com zoom** para exibir uma versão maior do gráfico em uma nova aba do navegador.
5. Veja os dois gráficos lado a lado e identifique as áreas onde os valores de IOPS parecem ser bem diferentes.
6. Mova o cursor sobre essas áreas para comparar o IOPS local e total para um ponto específico no tempo.

Componentes das páginas de destino do objeto

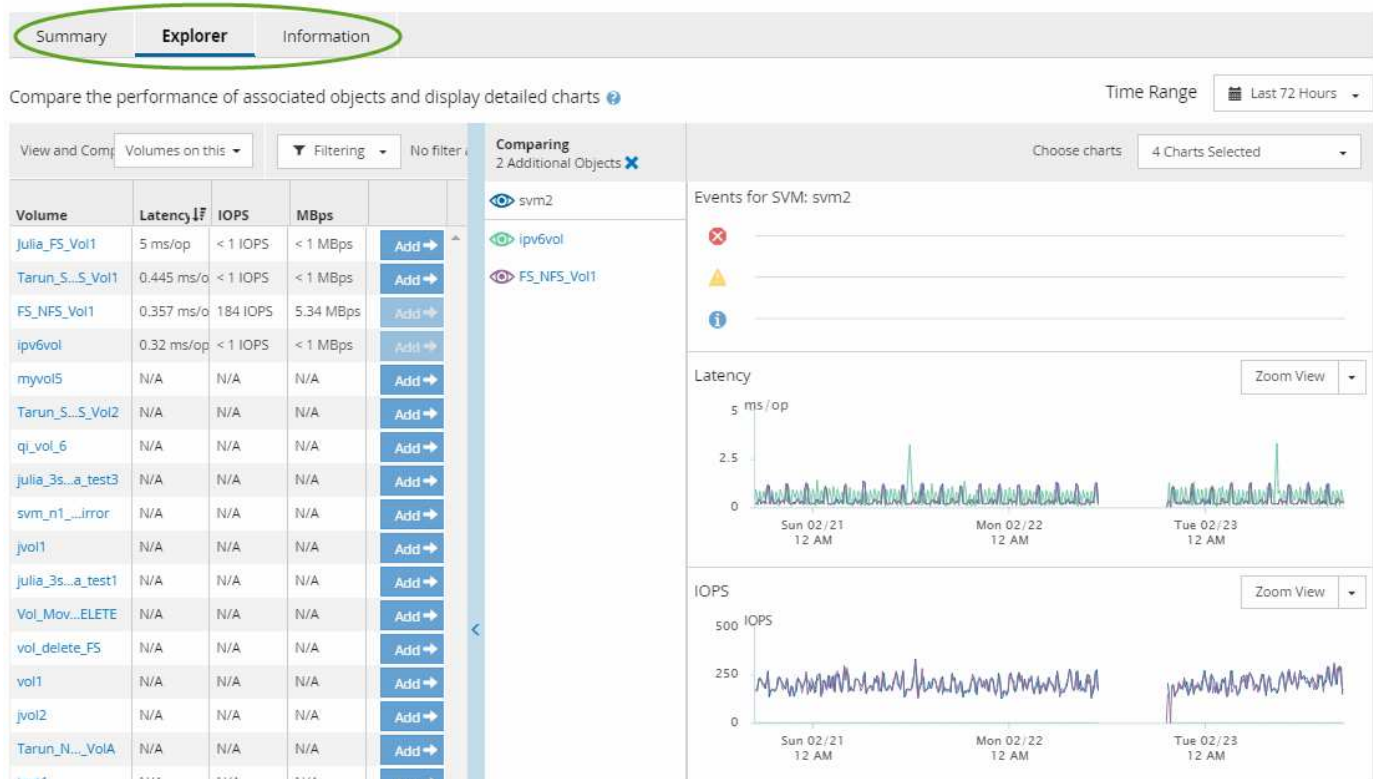
As páginas de destino do objeto fornecem detalhes sobre todos os eventos críticos, de aviso e informativos. Eles fornecem uma visão detalhada do desempenho de todos os objetos do cluster, permitindo que você selecione e compare objetos individuais em vários períodos de tempo.

As páginas de destino do objeto permitem que você examine o desempenho geral de todos os objetos e compare 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 exibidos nos painéis de resumo do contador e nos gráficos do contador são baseados em um 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 exibindo as informações do Explorer:



Dependendo do objeto de armazenamento que está sendo visualizado, a página Object Landing pode ter as seguintes guias que fornecem dados de desempenho sobre o objeto:

- Resumo

Exibe três ou quatro gráficos de contadores contendo os eventos e o desempenho por objeto no período de 72 horas anterior, incluindo uma linha de tendência que mostra os valores altos e baixos 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. Esta aba inclui até onze gráficos de contagem e um seletor de intervalo de tempo, que permitem que você realize uma variedade de comparações.

- Informação

Exibe valores para atributos de configuração sem desempenho sobre o objeto de armazenamento, incluindo a versão instalada do software ONTAP, nome do parceiro de HA e número de portas e LIFs.

- Melhores desempenhos

Para clusters: exibe os objetos de armazenamento que têm o maior ou menor desempenho, com base no contador de desempenho selecionado.

- Planejamento de Failover

Para nós: exibe a estimativa do impacto no desempenho de um nó se o parceiro de HA do nó falhar.

- **Detalhes**

Para volumes: exibe estatísticas detalhadas de desempenho para todas as atividades e operações de E/S para a carga de trabalho do volume selecionado. Esta guia está disponível para volumes FlexVol , volumes FlexGroup e constituintes de FlexGroups.

Página de resumo

A página Resumo exibe gráficos de contadores que contêm detalhes sobre os eventos e o desempenho por objeto no período de 72 horas anterior. Esses dados não são atualizados automaticamente, mas são atuais desde o 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 do último período de 72 horas e ajudam você a identificar possíveis problemas que exigem investigação adicional.

As estatísticas do contador da página Resumo são exibidas em gráficos.

Você pode posicionar o cursor sobre a linha de tendência em um gráfico para visualizar os valores do contador para um determinado momento. 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 objetos.

- **IOPS**

Velocidade média de operação; expressa em operações de entrada/saída por segundo.

Exibido para todos os tipos de objetos.

- **MB/s**

Taxa de transferência média; expressa em megabytes por segundo.

Exibido para todos os tipos de objetos.

- **Capacidade de Desempenho Utilizada**

Porcentagem da capacidade de desempenho que está sendo consumida por um nó ou agregado.

Exibido somente para nós e agregados.

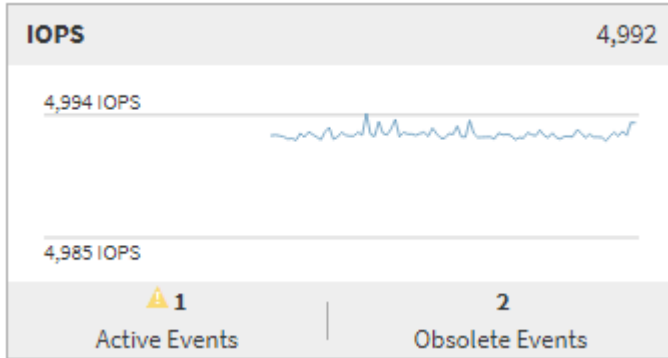
- **Utilização**

Porcentagem de utilização de objetos para nós e agregados, ou utilização de largura de banda para portas.

Exibido somente 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 linha de tendência são os valores mínimo e máximo do 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.



- **Gráfico do contador de latência**

O gráfico do contador de latência fornece uma visão geral de alto nível da latência do objeto no período anterior de 72 horas. Latência se refere ao tempo médio de resposta para todas as solicitações de E/S; expresso em milissegundos por operação, o tempo de serviço, o tempo de espera ou ambos experimentados por um pacote de dados ou bloco no componente de armazenamento do cluster em consideração.

Superior (valor do contador): O número no cabeçalho exibe a média do período anterior de 72 horas.

Meio (gráfico de desempenho): O número na parte inferior do gráfico exibe a menor latência, e o número na parte superior do gráfico exibe a maior latência do período anterior de 72 horas. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor de latência de 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 e visualizar detalhes completos do evento.

- **Gráfico do contador IOPS**

O gráfico do contador de IOPS fornece uma visão geral de alto nível da integridade do IOPS do objeto no período anterior de 72 horas. 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 anterior de 72 horas.

Meio (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 do período de 72 horas anterior. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor do IOPS para um período 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 e visualizar detalhes completos do evento.

- **Gráfico de contador MB/s**

O gráfico do contador MB/s exibe o desempenho do objeto em MB/s e indica quantos dados foram transferidos de e para o objeto em megabytes por segundo. O gráfico do contador MB/s fornece uma visão geral de alto nível da integridade de MB/s do objeto no período anterior de 72 horas.

Superior (valor do contador): O número no cabeçalho exibe a média de MB/s do período de 72 horas anterior.

Meio (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 no período de 72 horas anterior. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor de 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 e visualizar detalhes completos do evento.

- **Gráfico do contador de capacidade de desempenho utilizada**

O gráfico do 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 no período de 72 horas anterior.

Meio (gráfico de desempenho): O valor na parte inferior do gráfico exibe a menor porcentagem de capacidade de desempenho utilizada, e o valor na parte superior do gráfico exibe a maior porcentagem de capacidade de desempenho utilizada no período de 72 horas anterior. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor da capacidade de desempenho usada em um período 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 e visualizar detalhes completos do evento.

- **Gráfico de 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 de utilização do objeto ou da largura de banda no período anterior de 72 horas.

Superior (valor do contador): O número no cabeçalho exibe a porcentagem média de utilização do período de 72 horas anterior.

Meio (gráfico de desempenho): O valor na parte inferior do gráfico exibe a menor porcentagem de utilização, e o valor na parte superior do gráfico exibe a maior porcentagem de utilização do período de 72 horas anterior. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor de utilização de um período 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 e visualizar detalhes completos do evento.

Eventos

A tabela de histórico de eventos, quando aplicável, lista os eventos mais recentes que ocorreram naquele

objeto. Clicar no nome do evento exibe detalhes do evento na página Detalhes do evento.

Componentes da página do 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 contra a qual outras comparações de objetos são feitas.

Você pode clicar no botão **Alternar para a visualização de integridade** para exibir a página de detalhes de integridade deste objeto. Em alguns casos, você pode aprender informações importantes sobre as definições de configuração de armazenamento deste objeto que podem ajudar na solução de problemas.

A página Performance Explorer 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 do objeto) em um formato tabular. Esta 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 naquele objeto naquele momento.

A página Performance Explorer contém os seguintes componentes:

- **Intervalo de tempo**

Permite que você selecione 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 selecionar qual tipo de objeto correlacionado é exibido na grade.

As opções disponíveis dependem do tipo de objeto raiz e dos 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 que você restrinja a quantidade de dados recebidos, com base em 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 dos objetos no painel Comparação são exibidos nos Gráficos de Contadores.

- **Ver estatísticas em**

Para volume e LUNs, permite que você selecione se as estatísticas serão exibidas após cada ciclo de

coleta (padrão 5 minutos) ou se as estatísticas serão 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 Contagem**

Exibe dados gráficos para cada categoria de desempenho do objeto.

Normalmente, apenas três ou quatro gráficos são exibidos por padrão. O componente Escolher gráficos permite que você exiba gráficos adicionais ou oculte gráficos específicos. Você também pode optar por mostrar ou ocultar a Linha do tempo de eventos.

- **Cronograma dos eventos**

Exibe eventos de desempenho e integridade que ocorrem na linha do tempo selecionada no componente Intervalo de tempo.

Gerenciar desempenho usando informações do grupo de políticas de QoS

O Unified Manager permite que você visualize os grupos de políticas de qualidade de serviço (QoS) que estão disponíveis em todos os clusters que você está monitorando. As políticas podem ter sido definidas usando o software ONTAP (System Manager ou ONTAP CLI) ou pelas políticas de nível de serviço de desempenho do Unified Manager. O Unified Manager também exibe quais volumes e LUNs têm um grupo de política de QoS atribuído.

Para obter mais informações sobre como ajustar as configurações de QoS, consulte ["Visão geral da gestão de desempenho"](#)

Como o QoS de armazenamento pode controlar a taxa de transferência da carga de trabalho

Você pode criar um grupo de políticas de Qualidade de Serviço (QoS) para controlar o limite de E/S por segundo (IOPS) ou de taxa de transferência (MB/s) para as cargas de trabalho que ele contém. Se as cargas de trabalho estiverem em um grupo de políticas sem limite definido, como o grupo de políticas padrão, ou se 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.

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 total. Grupos de políticas de QoS também podem ser atribuídos a várias cargas de trabalho; nesse caso, o limite de taxa de transferência é "compartilhado" entre as cargas de trabalho. Por exemplo, um limite de QoS de 9.000 IOPS atribuído a três cargas de trabalho restringiria o IOPS combinado de exceder 9.000 IOPS.

Grupos de políticas de QoS "adaptáveis" também podem ser atribuídos a cargas de trabalho individuais ou a múltiplas cargas de trabalho. No entanto, mesmo quando atribuída a várias cargas de trabalho, cada carga de trabalho obtém o limite de taxa de transferência total em vez de compartilhar o valor de taxa de transferência com outras cargas de trabalho. Além disso, as políticas de QoS adaptáveis ajustam automaticamente a

configuração de taxa de transferência com base no tamanho do volume, por carga de trabalho, mantendo assim a proporção de IOPS para terabytes conforme o tamanho do volume muda. Por exemplo, se o pico for definido como 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, o QoS adaptável ajustará 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 efetivamente converte 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, por fim, usando uma grande porcentagem de taxa de transferência.

Para políticas de QoS de grupo compartilhado, quando o IOPS ou MB/s de todas as cargas de trabalho em um grupo de políticas excede o limite definido, o grupo de políticas limita as cargas de trabalho para restringir sua atividade, o que pode diminuir o desempenho de todas as cargas de trabalho 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, você pode selecionar outros volumes ou LUNs no volume para comparar com o uso de throughput de IOPS ou MBps da carga de trabalho afetada.

Ao atribuir as cargas de trabalho que estão usando excessivamente os recursos do nó a uma configuração de grupo de políticas mais restritiva, o grupo de políticas limita as cargas de trabalho para restringir sua atividade, o que pode reduzir o uso dos recursos naquele 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 System Manager, os comandos ONTAP ou os Níveis de Serviço de Desempenho do Unified Manager para gerenciar grupos de políticas, incluindo as seguintes tarefas:

- Criando um grupo de políticas
- Adicionar ou remover cargas de trabalho em um grupo de políticas
- Movendo uma carga de trabalho entre grupos de políticas
- Alterando o limite de taxa de transferência de um grupo de políticas
- Mover uma carga de trabalho para um agregado e/ou nó diferente

Exibir todos os grupos de políticas de QoS disponíveis em todos os clusters

Você pode exibir uma lista de todos os grupos de políticas de QoS disponíveis nos clusters que o Unified Manager está monitorando. Isso inclui políticas de QoS tradicionais, políticas de QoS adaptáveis e políticas de QoS gerenciadas por políticas de nível de serviço de desempenho do Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Grupos de políticas de QoS**.

A exibição Desempenho: Grupos de políticas de QoS tradicionais é exibida por padrão.

2. Veja as configurações detalhadas para 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 visualizar todos os grupos de políticas de QoS adaptáveis ou para visualizar todos os grupos de políticas de QoS que foram criados usando os Níveis de Serviço de Desempenho do Unified Manager.

Exibir volumes ou LUNs que estão no mesmo grupo de política de QoS

Você pode exibir uma lista dos volumes e LUNs que foram 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 verificar se determinados volumes estão usando em excesso a taxa de transferência definida para o grupo de políticas. Isso também pode ajudar você a decidir se 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 Desempenho do Unified Manager, pode ser útil visualizar todos os volumes ou LUNs que estão usando um grupo de políticas para que você possa ver quais objetos seriam afetados se você alterasse as configurações da política de QoS.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Grupos de políticas de QoS**.

A exibição Desempenho: Grupos de políticas de QoS tradicionais é exibida por padrão.

2. Se você estiver interessado em grupos de políticas tradicionais, continue nesta página. Caso contrário, selecione uma das opções adicionais de Exibição para exibir todos os grupos de políticas de QoS adaptáveis ou todos os grupos de políticas de QoS que foram 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 Política de QoS para ver mais detalhes.

Quality of Service - Performance / Adaptive QoS Policy Groups ?

Last updated: Jan 31, 2019, 1:56 PM ↻

View Adaptive QoS Policy Groups Search Quality of Service

Schedule Report								
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	
Details								
Allocated Capacity 0.99 TB 1.15 TB								
Associated Objects 2 Volumes 0 LUNs								
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 visualizar os objetos que usam esta política de QoS.

A página Inventário de desempenho para volumes ou LUNs é exibida com a lista classificada de objetos que estão usando a política de QoS.

Visualize as configurações do grupo de políticas de QoS aplicadas a volumes ou LUNs específicos

Você pode visualizar os grupos de políticas de QoS que foram aplicados aos seus volumes e LUNs e pode vincular à exibição Grupos de políticas de desempenho/QoS para exibir as configurações detalhadas de cada política de QoS.

As etapas para visualizar a política de QoS aplicada a um volume são mostradas abaixo. As etapas para visualizar essas informações para um LUN são semelhantes.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.

A visualização Saúde: Todos os volumes é exibida por padrão.

2. No menu Exibir, selecione **Desempenho: Volumes no Grupo de Políticas de QoS**.
3. Localize o volume que você deseja revisar e role para a direita até ver a coluna **Grupo de política de QoS**.
4. Clique no nome do Grupo de Políticas de QoS.

A página Qualidade de 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. Veja as configurações detalhadas para o 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.

Visualize 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 políticas 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 visualizar essas informações para um LUN são semelhantes.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.

A visualização Saúde: Todos os volumes é exibida por padrão.

2. No menu Exibir, selecione **Desempenho: Volumes no Grupo de Políticas de QoS**.
3. Clique no nome do volume que você deseja revisar.

A página Performance Explorer é exibida 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 IOPS, MB/s, IOPS/TB e outros contadores de desempenho para todos os volumes selecionados nos gráficos.

Você pode alterar o intervalo de tempo para visualizar o desempenho em intervalos de tempo diferentes do padrão de 72 horas.

Como diferentes tipos de políticas de QoS são exibidos nos gráficos de taxa de transferência

Você pode visualizar as configurações de política de qualidade de serviço (QoS) definidas ONTAP que foram aplicadas a um volume ou LUN nos gráficos IOPS, IOPS/TB e MB/s do Performance Explorer e da Análise de Carga de Trabalho. 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, portanto, limita o impacto em cargas de trabalho concorrentes pelos recursos do sistema. Uma configuração de taxa de transferência mínima (ou "esperada") define a taxa de transferência mínima que deve estar disponível para a carga de trabalho para que uma carga de trabalho crítica atinja as metas de taxa de transferência mínima, independentemente da demanda de cargas de trabalho concorrentes.

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 de QoS adaptáveis 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 elas são aplicadas às cargas de trabalho, há três maneiras pelas quais a política de QoS será exibida nos gráficos de desempenho.

Tipo de política	Funcionalidade	Indicador na interface do Unified Manager
Política compartilhada de QoS atribuída a uma única carga de trabalho ou política não compartilhada de QoS atribuída a uma única carga de trabalho ou a várias cargas de trabalho	Cada carga de trabalho pode consumir a configuração de taxa de transferência especificada	Exibe "(QoS)"
Política compartilhada de QoS atribuída a várias cargas de trabalho	Todas as cargas de trabalho compartilham a configuração de taxa de transferência especificada	Exibe "(QoS Compartilhado)"
Política de QoS adaptável atribuída a uma única carga de trabalho ou a várias cargas de trabalho	Cada carga de trabalho pode consumir a configuração de taxa de transferência especificada	Exibe "(QoS Adaptável)"

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 de IOPS/TB para uma carga de trabalho, o ONTAP converte o valor de IOPS em um valor de IOPS/TB e o Unified Manager exibe essa política no gráfico de IOPS/TB junto com o texto “QoS, definida 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 junto com o texto “QoS Adaptável - Usado, definido em IOPS/TB” ou “QoS Adaptável - Alocado, definido em IOPS/TB”, dependendo de como a configuração de alocação de pico de IOPS está configurada. Quando a configuração de alocação é definida como “allocated-space”, o pico de IOPS é calculado com base no tamanho do volume. Quando a configuração de alocação é definida como “used-space”, o pico de IOPS é calculado com base na quantidade de dados armazenados no volume, levando em consideração a eficiência 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 utilizada cai abaixo de 128 GB durante o período selecionado.

Visualize as configurações mínimas e máximas de QoS da carga de trabalho no Performance Explorer

Você pode visualizar as configurações de política de qualidade de serviço (QoS) definidas ONTAP em um volume ou LUN nos gráficos do Performance Explorer. Uma configuração de taxa de transferência máxima limita o impacto de cargas de trabalho concorrentes nos recursos do sistema. Uma configuração mínima de taxa de transferência garante que uma carga de trabalho crítica atinja metas mínimas de taxa de transferência, independentemente da demanda de cargas de trabalho concorrentes.

As configurações de IOPS e MB/s de taxa de transferência de QoS “mínimo” e “máximo” são exibidas nos gráficos de contadores somente se tiverem sido configuradas no ONTAP. As configurações mínimas de taxa de transferência estão disponíveis somente em sistemas que executam o software ONTAP 9.2 ou posterior, somente em sistemas AFF, e podem ser definidas somente para IOPS no momento.

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 carga de trabalho, mantendo assim a proporção de IOPS para terabytes conforme o tamanho do volume muda. Você pode aplicar um grupo de políticas de QoS adaptável somente a volumes. A terminologia de QoS “esperado” e “pico” é usada para políticas de QoS adaptáveis em vez de mínimo e máximo.

O Unified Manager gera eventos de aviso para violações de política de QoS quando a taxa de transferência de carga de trabalho excede a configuração máxima de política de QoS definida durante cada período de coleta de desempenho da hora anterior. A taxa de transferência da carga de trabalho 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 mesmo que a taxa de transferência de uma carga de trabalho não tenha ultrapassado o limite da política mostrado no gráfico.

Passos

- 1. Na página **Performance Explorer** do volume ou LUN selecionado, execute as seguintes ações para visualizar as configurações de teto e piso de QoS:

Se você quiser...	Faça isso...
Veja o teto de IOPS (o QoS máximo)	No gráfico Total ou Detalhamento do IOPS, clique em Visualização com Zoom .
Veja o teto de MB/s (QoS máximo)	No gráfico Total ou Detalhamento de MB/s, clique em Visualização com Zoom .
Veja o piso IOPS (o QoS mínimo)	No gráfico Total ou Detalhamento do IOPS, clique em Visualização com Zoom .
Veja o teto de IOPS/TB (o pico de QoS)	Para volumes, no gráfico IOPS/TB, clique em Visualização com zoom .
Visualizar o piso IOPS/TB (a QoS esperada)	Para volumes, no gráfico IOPS/TB, clique em Visualização com zoom .

A linha tracejada horizontal indica o valor máximo ou mínimo de taxa de transferência definido no ONTAP. Você também pode ver quando as alterações nos valores de QoS foram implementadas.

- 2. Para visualizar os valores específicos de IOPS e MB/s 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 determinados volumes ou LUNs têm IOPS ou MB/s muito altos e estão sobrecarregando os recursos do sistema, você pode usar o Gerenciador do Sistema ou a CLI do ONTAP para ajustar as configurações de QoS para que essas cargas de trabalho não afetem o desempenho de outras cargas de trabalho.

Para obter mais informações sobre como ajustar as configurações de QoS, consulte ["Visão geral da gestão de desempenho"](#)

Gerencie o desempenho usando a capacidade de desempenho e as informações de IOPS disponíveis

Capacidade de desempenho indica quanta produtividade você pode obter de um recurso

sem ultrapassar o desempenho útil desse recurso. Quando visualizada usando contadores de desempenho existentes, a capacidade de desempenho 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 desempenho de nós e agregados em cada cluster. *Capacidade de desempenho utilizada* é a porcentagem da capacidade de desempenho que está sendo usada atualmente, e *capacidade de desempenho livre* é a porcentagem da capacidade de desempenho que ainda está disponível.

Enquanto a capacidade de desempenho livre fornece 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. Ao usar essa métrica, você pode ter certeza de que pode adicionar cargas de trabalho de um número predeterminado de IOPS a um recurso.

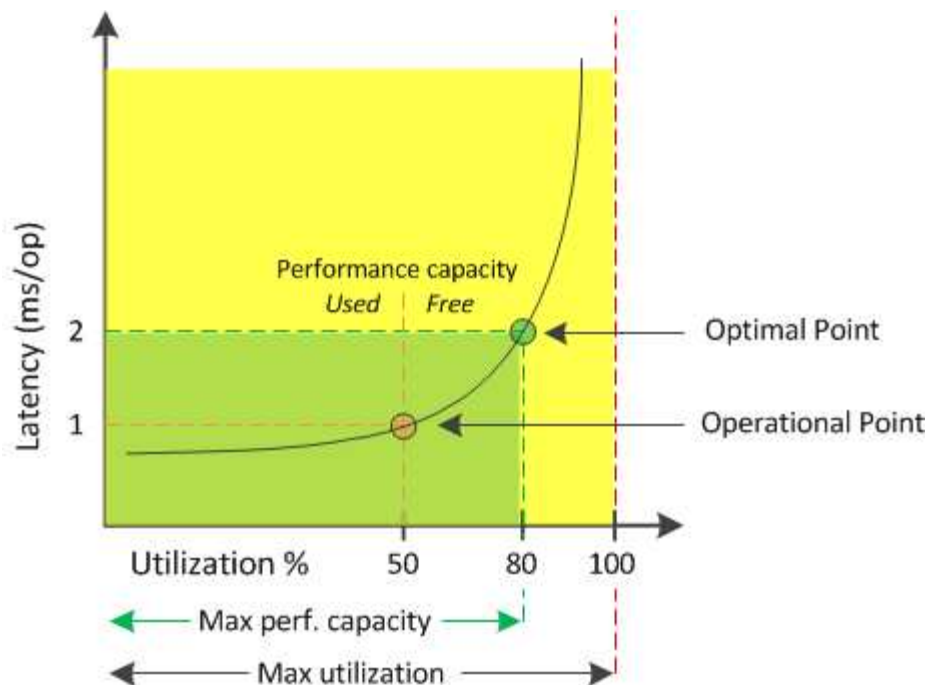
Monitorar as informações de capacidade de desempenho tem os seguintes benefícios:

- Auxilia no provisionamento e balanceamento do fluxo de trabalho.
- Ajuda a evitar a sobrecarga de um nó ou o uso excessivo de seus recursos além do ponto ideal, reduzindo assim a necessidade de solução de 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 usada ajuda a identificar se o desempenho de um nó ou de um agregado está atingindo um ponto em que o desempenho pode diminuir 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 desempenho utilizada é semelhante à utilização, mas a primeira fornece mais informações sobre os recursos de desempenho disponíveis em um recurso físico para uma carga de trabalho específica.

A capacidade de desempenho ideal utilizada é o ponto em que um nó ou um agregado tem utilização e latência ideais (tempo de resposta) e está sendo usado de forma eficiente. 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 com 50% de utilização, com latência de 1,0 ms/op. Com base nas estatísticas capturadas do agregado, o Unified Manager determina que capacidade de desempenho adicional está disponível para esse agregado. Neste exemplo, o *ponto ideal* é identificado como o ponto em que o agregado está com 80% de utilização com latência de 2,0 ms/op. Portanto, você pode adicionar mais volumes e LUNs a esse agregado para que seus sistemas sejam usados de forma mais eficiente.

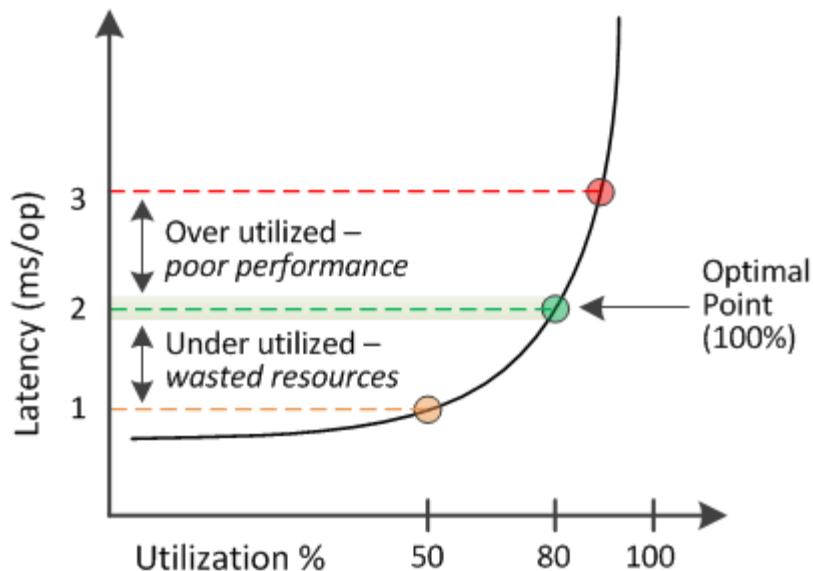
Espera-se que o contador de capacidade de desempenho utilizada seja um número maior que o contador de “utilização” porque a capacidade de desempenho adiciona impacto na latência. Por exemplo, se um nó ou agregado estiver 70% utilizado, o valor da capacidade de desempenho pode estar na faixa de 80% a 100%, dependendo do valor de latência.

Em alguns casos, no entanto, o contador de utilização pode ser maior na página do Painel. Isso é normal porque o painel atualiza os valores atuais do contador em cada período de coleta; ele não exibe médias ao longo de um período de tempo como as outras páginas na interface do usuário do Unified Manager. O contador de capacidade de desempenho utilizada é melhor utilizado como um indicador de desempenho médio ao longo de um período de tempo, enquanto o contador de utilização é melhor utilizado para determinar o uso instantâneo de um recurso.

O que significa o valor da capacidade de desempenho utilizada

O valor da capacidade de desempenho usada ajuda a identificar os nós e agregados que estão sendo superutilizados ou subutilizados. Isso permite que você redistribua cargas de trabalho para tornar seus recursos de armazenamento mais eficientes.

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 pode estar localizado.



- Uma percentagem de capacidade de desempenho utilizada igual a 100 está no ponto ideal.

Os recursos estão sendo usados eficientemente neste momento.

- Uma percentagem de capacidade de desempenho utilizada acima de 100 indica que o nó ou agregado está superutilizado 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 utilizada abaixo de 100 indica que o nó ou agregado está subutilizado e que os recursos não estão sendo usados de forma eficaz.

Mais cargas de trabalho podem ser adicionadas ao recurso.



Diferentemente da utilização, a percentagem de capacidade de desempenho utilizada pode ser superior a 100%. Não há uma percentagem máxima, mas os recursos normalmente estarão na faixa de 110% a 140% quando estão sendo superutilizados. Porcentagens mais altas indicariam um recurso com problemas sérios.

O que é IOPS disponível

O contador de IOPS disponíveis identifica o número restante de IOPS que podem ser adicionados a um nó ou agregado antes que o recurso atinja seu limite.

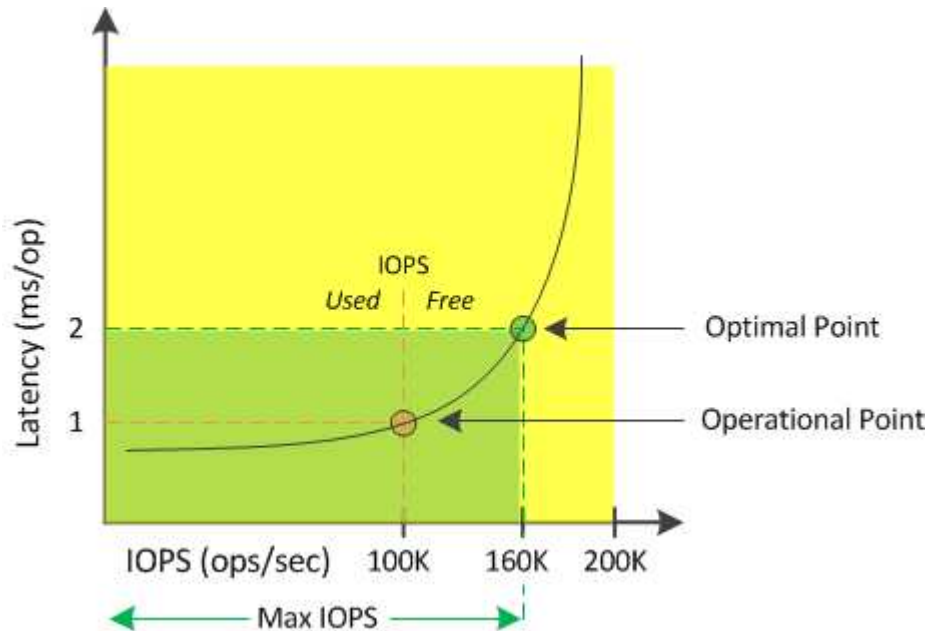
O IOPS total que um nó pode fornecer é baseado nas características físicas do nó — por exemplo, o número de CPUs, a velocidade da CPU e a quantidade de RAM. O IOPS total que um agregado pode fornecer é baseado nas propriedades físicas dos discos, por exemplo, um disco SATA, SAS ou SSD.

O IOPS total de todos os volumes em um agregado pode não corresponder ao IOPS total 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?"](#)

Enquanto o contador de capacidade de desempenho livre fornece a percentagem de um recurso que ainda está disponível, o contador de IOPS disponíveis informa o número exato de IOPS (cargas de trabalho) que podem ser adicionadas a um recurso antes de atingir a capacidade máxima de desempenho.

Por exemplo, se você estiver usando um par de sistemas de armazenamento FAS2520 e FAS8060, um valor de capacidade de desempenho livre de 30% significa que você tem alguma capacidade de desempenho livre. No entanto, esse valor não fornece visibilidade sobre quantas cargas de trabalho adicionais você pode implantar nesses nós. O contador de IOPS disponíveis pode mostrar que você tem 500 IOPS disponíveis no FAS8060, mas apenas 100 IOPS disponíveis no FAS2520.

Uma curva de latência versus IOPS de exemplo 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 está em 100% (o ponto ideal). O ponto operacional identifica que o nó está operando atualmente a 100K IOPS com latência de 1,0 ms/op. Com base nas estatísticas capturadas do nó, o Unified Manager determina que o IOPS máximo para o nó é 160K, o que significa que há 60K IOPS livres ou disponíveis. Portanto, você pode adicionar mais cargas de trabalho a este nó para que seus sistemas sejam usados de forma mais eficiente.



Quando há atividade mínima do usuário no recurso, o valor de IOPS disponível é calculado assumindo uma carga de trabalho genérica baseada em aproximadamente 4.500 IOPS por núcleo de CPU. Isso ocorre porque o Unified Manager não possui dados para estimar com precisão as características da carga de trabalho que está sendo atendida.

Exibir valores usados de capacidade de desempenho de nó e agregado

Você pode monitorar os valores de capacidade de desempenho usados para todos os nós ou para todos os agregados em um cluster, ou pode visualizar detalhes de um único nó ou agregado.

Os valores usados na capacidade de desempenho aparecem no Painel, nas páginas Inventário de desempenho, na página Melhores desempenhos, na página Criar política de limite, nas páginas do Explorador de desempenho e em gráficos detalhados. Por exemplo, a página Desempenho: Todos os agregados fornece uma coluna Capacidade de desempenho usada para visualizar 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

Filtering No filter applied Search Aggregates Data Search												
Assign Threshold Policy Clear Threshold Policy												
☐	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

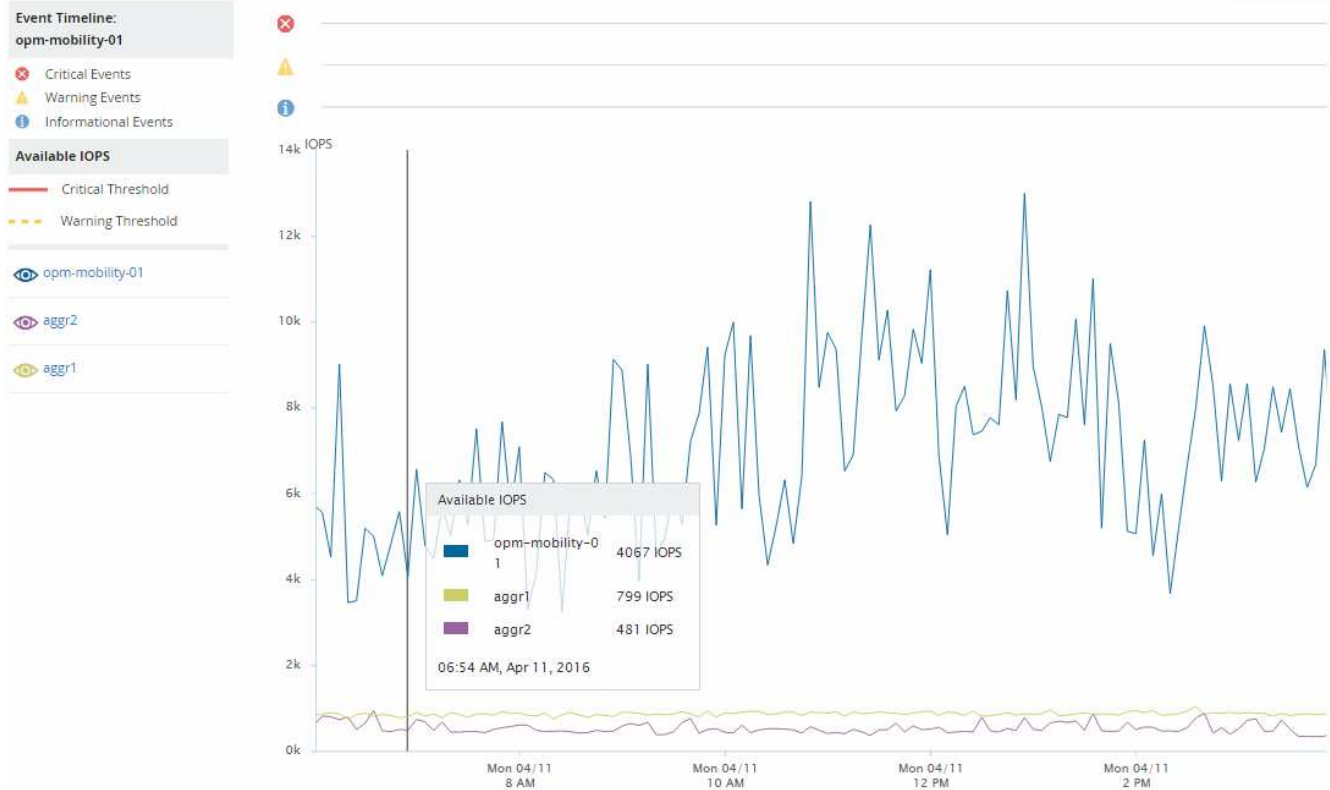
Monitorar a capacidade de desempenho utilizada pelo contador permite identificar o seguinte:

- Se algum nó ou agregado em algum cluster tem um valor de capacidade de alto desempenho usado
- Se algum nó ou agregado em algum cluster tem eventos de capacidade de desempenho ativa usados
- Os nós e agregados que têm o maior e o menor valor de capacidade de desempenho usado em um cluster
- Valores de contador de latência e utilização em conjunto com nós ou agregados que têm valores usados de alta capacidade de desempenho
- Como os valores de capacidade de desempenho usados para nós em um par HA serão afetados se um dos nós falhar
- Os volumes e LUNs mais movimentados em um agregado que tem um alto valor de capacidade de desempenho usado

Exibir valores de IOPS disponíveis para nós e agregados

Você pode monitorar os valores de IOPS disponíveis para todos os nós ou para todos os agregados em um cluster, ou pode visualizar detalhes de um único nó ou agregado.

Os valores de IOPS disponíveis aparecem nas páginas de Inventário de Desempenho e nos gráficos da página do Explorador de Desempenho para nós e agregados. Por exemplo, ao visualizar um nó na página Node/Performance Explorer, você pode selecionar o gráfico de contador "IOPS disponíveis" na lista para poder comparar os valores de IOPS disponíveis para o nó e vários agregados naquele nó.



Monitorar o contador de IOPS disponível permite que você identifique:

- Os nós ou agregados que têm os maiores valores de IOPS disponíveis para ajudar a determinar onde futuras cargas de trabalho podem ser implantadas.
- 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 movimentados em um agregado que tem um pequeno valor de IOPS disponível.

Visualize gráficos de contadores de capacidade de desempenho para identificar problemas

Você pode visualizar gráficos de capacidade de desempenho usada para nós e agregados na página Performance Explorer. Isso permite que você visualize dados detalhados de capacidade de desempenho para os nós e agregados selecionados 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 do contador de detalhamento exibe os valores totais de capacidade de desempenho para o objeto raiz separados por uso com base nos protocolos do usuário versus processos do sistema em segundo plano. Além disso, a quantidade de capacidade de desempenho livre também é mostrada.

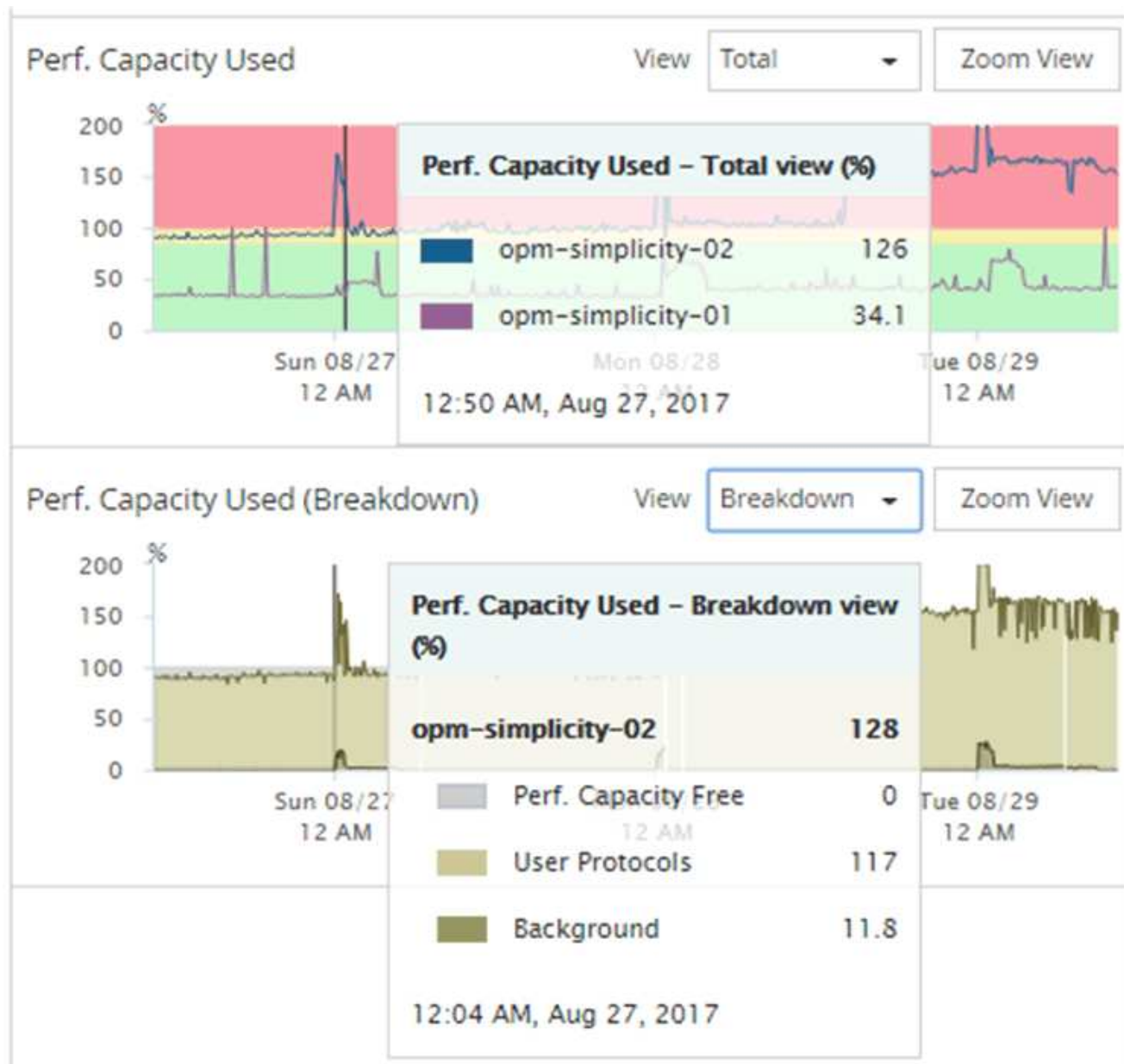


Como algumas atividades em segundo plano associadas ao gerenciamento de sistemas e dados são identificadas como cargas de trabalho do usuário e categorizadas como protocolos do usuário, a porcentagem de protocolos do usuário pode parecer artificialmente alta quando esses processos são executados. Esses processos geralmente são executados por volta da meia-noite, quando o uso do cluster é baixo. Se você observar 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 naquele horário.

Passos

1. Selecione a aba **Explorer** de um nó ou página de destino agregada.
2. No painel **Gráficos do contador**, clique em **Escolher gráficos** e selecione **Desempenho. Gráfico de Capacidade Utilizada**.
3. Role para baixo até conseguir visualizar o gráfico.

As cores do gráfico padrão mostram quando o objeto está na faixa ideal (amarelo), quando o objeto está subutilizado (verde) e quando o objeto está superutilizado (vermelho). O gráfico de detalhamento mostra detalhes detalhados da capacidade de desempenho somente para o objeto raiz.



4. Se você quiser visualizar qualquer um dos gráficos em tamanho real, clique em **Visualização com Zoom**.

Dessa forma, você pode abrir vários gráficos de contadores em janelas separadas para comparar valores de capacidade de desempenho usados com valores de IOPS ou MBps no mesmo período.

Capacidade de desempenho usada em condições de limiar de desempenho

Você pode criar políticas de limite de desempenho definidas pelo usuário para que eventos sejam acionados quando o valor de capacidade de desempenho usada para um nó ou agregado exceder a configuração de limite de capacidade de desempenho usada definida.

Além disso, os nós podem ser configurados com uma política de limite de “Aquisição de capacidade de desempenho usada”. Esta política de limite totaliza as estatísticas de capacidade de desempenho usadas para ambos os nós em um par de HA para determinar se um dos nós não teria capacidade suficiente se o outro nó falhasse. Como a carga de trabalho durante o failover é a combinação das cargas de trabalho dos

dois nós parceiros, a mesma política de aquisição de capacidade de desempenho usada pode ser aplicada a ambos os nós.



Essa equivalência de capacidade de desempenho usada geralmente é 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 de desempenho total usada ao executar todas as cargas de trabalho em um nó parceiro em comparação ao outro nó parceiro poderá ser ligeiramente diferente dependendo de qual nó falhou.

As condições de capacidade de desempenho usadas também podem ser usadas como configurações de limite de desempenho 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 o volume ou LUN reside. Por exemplo, você pode criar uma política de limite de combinação usando os seguintes critérios:

Objeto de armazenamento	Contador de desempenho	Limite de alerta	Limiar crítico	Duração
Volume	Latência	15 ms/operação	25 ms/op	20 minutos
Agregar	Capacidade de desempenho utilizada	80%	95%	

Políticas de limite de combinação fazem com que um evento seja gerado somente quando ambas as condições são violadas durante toda a duração.

Use o contador de capacidade de desempenho usado para gerenciar o desempenho

Normalmente, as organizações desejam operar com uma porcentagem de capacidade de desempenho utilizada abaixo de 100 para que os recursos sejam usados de forma eficiente, ao mesmo tempo em que reservam alguma capacidade de desempenho adicional para dar suporte às demandas dos períodos de pico. Você pode usar políticas de limite para personalizar quando os alertas são enviados para valores de alta capacidade de desempenho utilizados.

Você pode estabelecer metas específicas com base em seus requisitos de desempenho. Por exemplo, empresas de serviços financeiros podem reservar mais capacidade de desempenho para garantir a execução oportuna das negociações. Essas empresas podem querer definir limites de capacidade de desempenho usados na faixa de 70-80 por cento. 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 utilizados na faixa de 85-95 por cento.

Quando o valor da capacidade de desempenho 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 problemas potenciais antes que eles afetem o desempenho. Esses eventos também podem ser usados como indicadores de que você precisa fazer movimentações e alterações na carga de trabalho em seus nós e agregados.

Entenda e use a página de planejamento de failover de nó

A página Planejamento de desempenho/failover de nó estima o impacto no desempenho de um nó se o nó parceiro de alta disponibilidade (HA) do nó falhar. O Unified Manager baseia as estimativas no desempenho histórico dos nós no par HA.

Estimar o impacto de um failover no desempenho ajuda você a planejar nos seguintes cenários:

- Se um failover degradar consistentemente o desempenho estimado do nó de aquisição a 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 para determinar o melhor momento para executar a tarefa.

Use 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 no desempenho de um failover, você pode mover alguns volumes ou LUNs de um nó no par HA para outros nós no cluster. Isso garante que o nó primário possa continuar a oferecer 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 Comparação. Essas seções permitem que você avalie o impacto de um failover de nó no desempenho do nó de aquisição.

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 utilizada.



Os valores de latência e IOPS exibidos nesta página e na página Desempenho/Explorador de Desempenho do Nó 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 lugar do 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 primário. As estatísticas de desempenho exibidas para este nó mostram o desempenho do nó de aquisição depois que ele assume o parceiro com falha.



Embora a carga de trabalho do nó de aquisição seja equivalente às cargas de trabalho combinadas de ambos os nós após um failover, as estatísticas do nó de aquisição estimada não são a soma das estatísticas do nó primário e do nó parceiro. Por exemplo, se a latência do nó primário for de 2 ms/op e a latência do nó parceiro for de 3 ms/op, o nó de aquisição estimada poderá ter uma latência de 4 ms/op. Este valor é um cálculo realizado 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 **Failover Planning** para ver como o desempenho muda neste cenário de falha de nó. Por exemplo, se o Nó1 for o nó primário e o Nó2 for o nó parceiro, você pode clicar no Nó2 para torná-lo o nó primário. Dessa forma, você pode ver como o desempenho estimado muda dependendo de qual nó falha.

Painel de comparação

A lista a seguir descreve os componentes exibidos no painel Comparação por padrão:

- **Gráficos de eventos**

Eles são exibidos no mesmo formato daqueles na página Performance/Node Performance Explorer. Elas pertencem somente ao nó primário.

- **Gráficos de contador**

Eles exibem estatísticas históricas para o contador de desempenho mostrado na grade. Em cada gráfico, o gráfico do nó Estimated Takeover mostra o desempenho estimado se um failover tivesse ocorrido em um determinado momento.

Por exemplo, suponha que o gráfico de Utilização mostre 73% para o nó de Aquisição Estimada às 11h do dia 8 de fevereiro. Se um failover tivesse ocorrido naquele momento, a utilização do nó de aquisição teria sido 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 somente em momentos em que o desempenho previsto do nó de aquisição for aceitável.

Por padrão, as estatísticas do objeto raiz e do nó parceiro são exibidas no painel Comparação. Diferentemente da página Performance/Node Performance Explorer, esta página não exibe o botão **Adicionar** para você adicionar objetos para comparação de estatísticas.

Você pode personalizar o painel Comparação da mesma forma que faz na página Desempenho/Explorador de Desempenho do Nó. 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 **Visualização com Zoom** para exibir um gráfico detalhado de um contador específico em uma nova janela.

Use uma política de limite com a página Planejamento de Failover de Nó

Você pode criar uma política de limite de nó para ser notificado na página Planejamento de failover de desempenho/nó quando um possível failover degradar o desempenho do nó de aquisição a um nível inaceitável.

A política de limite de desempenho definida pelo sistema, denominada “Par de HA de nós superutilizado”, 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 desempenho combinada usada pelos nós em um par HA exceder 200%.

O evento da política de limite definida pelo sistema alerta você sobre o fato de que um failover fará com que a latência do nó de aquisição aumente para um nível inaceitável. Ao ver um evento gerado por esta política para um nó específico, você pode navegar até a página Planejamento de failover de desempenho/nó desse nó para visualizar 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 menor que 200% permite que você receba um evento antes que o limite da política definida pelo sistema seja violado. Você também pode especificar o período mínimo de tempo durante o qual o limite será 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 de desempenho combinada usada pelos nós em um par de HA exceder 175% por mais de 10 minutos. Você pode aplicar essa política ao Node1 e Node2, que formam um par de HA. Após receber uma notificação de evento de aviso para o Nó 1 ou Nó 2, você pode visualizar a página Planejamento de failover de desempenho/nó para esse nó para avaliar o impacto estimado no desempenho do nó de aquisição. Você pode tomar ações corretivas para evitar sobrecarregar o nó de aquisição caso ocorra um failover. Se você tomar uma ação quando a capacidade de desempenho combinada usada pelos nós estiver abaixo de 200%, a latência do nó de aquisição não atingirá um nível inaceitável, mesmo que ocorra um failover durante esse período.

Use o gráfico de detalhamento da capacidade de desempenho usada para planejamento de failover

O gráfico detalhado de Capacidade de Desempenho Usada - Detalhamento mostra a capacidade de desempenho usada para o nó primário e o nó parceiro. Ele também mostra a quantidade de capacidade de desempenho livre no nó Estimated Takeover. Essas informações ajudam a determinar se você pode ter um problema de desempenho se o nó parceiro falhar.

Além de mostrar a capacidade total de desempenho usada pelos nós, o gráfico Detalhamento divide os valores de cada nó em protocolos de usuário e processos em segundo plano.

- Os protocolos do usuário são as operações de E/S dos aplicativos do usuário para e do cluster.
- Os processos em segundo plano são os processos internos do sistema envolvidos com a eficiência do armazenamento, a replicação de dados e a integridade do sistema.

Esse nível adicional de detalhes permite que você determine se um problema de desempenho é causado pela atividade do aplicativo do usuário ou por processos do sistema em segundo plano, como desduplicação, reconstrução de RAID, limpeza de disco e cópias do SnapMirror .

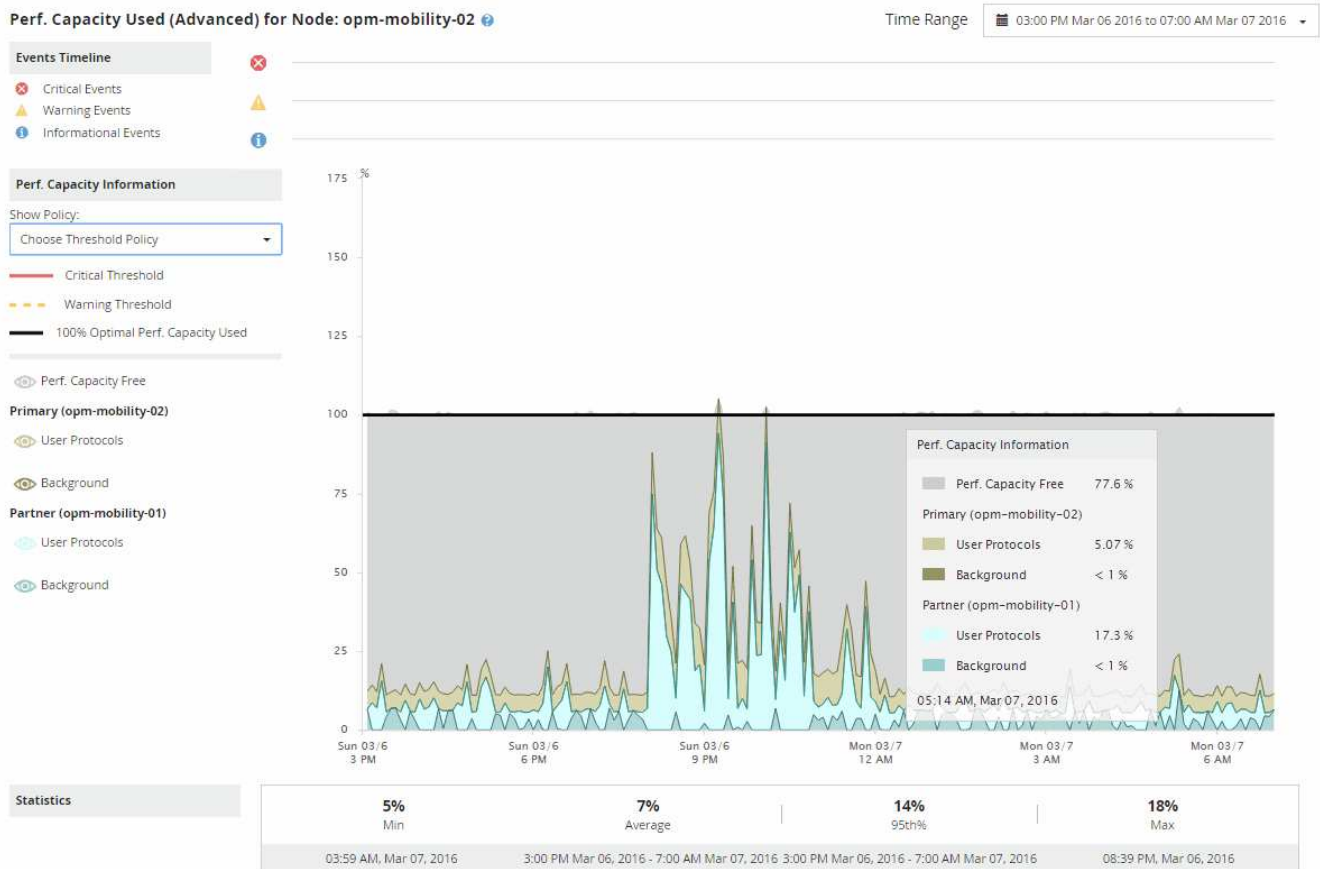
Passos

1. Acesse a página **Desempenho/Planejamento de failover de nó** para o nó que servirá como nó de aquisição estimada.
2. No seletor **Intervalo de tempo**, escolha o período de tempo para o qual as estatísticas históricas serão exibidas na grade do contador e nos gráficos do contador.

Os gráficos de contador com estatísticas para o nó primário, nó parceiro e nó de aquisição estimada são exibidos.

3. Na lista **Escolher gráficos**, selecione **Perf. Capacidade Utilizada**.
4. No **Perf. No gráfico Capacidade Utilizada**, selecione **Detalhamento** e clique em **Visualização com Zoom**.

O gráfico detalhado para Perf. A capacidade utilizada é exibida.



5. Mova o cursor sobre o gráfico detalhado para visualizar as informações de capacidade de desempenho utilizada na janela pop-up.

O Perf. A porcentagem de capacidade livre é a capacidade de desempenho disponível no nó de aquisição estimada. Indica quanta capacidade de desempenho resta no nó de aquisição após um failover. Se for 0%, um failover fará com que a latência aumente para um nível inaceitável no nó de aquisição.

6. Considere tomar ações corretivas para evitar uma baixa porcentagem de capacidade livre de desempenho.

Se você planeja iniciar um failover para manutenção do nó, escolha um momento para falhar o nó parceiro quando a porcentagem de capacidade livre de desempenho não estiver em 0.

Coletar dados e monitorar o desempenho da carga de trabalho

O Unified Manager coleta e analisa a atividade da carga de trabalho a cada 5 minutos para identificar eventos de desempenho e detecta alterações de configuração a cada 15 minutos. Ele retém no máximo 30 dias de dados históricos de desempenho e eventos de 5 minutos e usa esses dados para prever o intervalo de latência esperado para todas as cargas de trabalho monitoradas.

O Unified Manager deve coletar no mínimo 3 dias de atividade de carga de trabalho antes de poder iniciar sua análise e antes que a previsão de latência para o tempo de resposta de E/S possa ser exibida na página Análise de Carga de Trabalho e na página 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 00:00, para refletir as alterações na atividade da carga de trabalho e estabelecer um limite de desempenho dinâmico mais preciso.

Durante os primeiros 4 dias em que o Unified Manager estiver monitorando uma carga de trabalho, se mais de 24 horas tiverem se passado desde a última coleta de dados, os gráficos de latência não exibirão a previsão de latência para essa carga de trabalho. Os eventos detectados antes da última coleta 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, o que leva aproximadamente 15 dias para ser concluído. Durante esse período, você pode continuar a usar o Unified Manager, mas, como o Unified Manager usa a previsão de latência para detectar eventos dinâmicos, alguns eventos podem não ser precisos. Eventos detectados antes da mudança de horário não são afetados.

Tipos de cargas de trabalho monitoradas pelo Unified Manager

Você pode usar o Unified Manager para monitorar o desempenho de dois tipos de cargas de trabalho: definidas pelo usuário e definidas pelo sistema.

• Cargas de trabalho definidas pelo usuário

A taxa de transferência de E/S dos aplicativos para o cluster. Esses são processos envolvidos em solicitações de leitura e gravação. Um volume, LUN, compartilhamento NFS, compartilhamento SMB/CIFS e uma carga de trabalho são cargas de trabalho definidas pelo usuário.



O Unified Manager monitora apenas a atividade da carga de trabalho no cluster. Ele não monitora os aplicativos, os clientes ou os caminhos entre os aplicativos e o cluster.

Se uma ou mais das seguintes condições forem verdadeiras para uma carga de trabalho, ela não poderá ser monitorada pelo Unified Manager:

- É uma cópia de proteção de dados (DP) em modo somente leitura. (Os volumes DP são monitorados para tráfego gerado pelo usuário.)
- É um clone de dados offline.
- É um volume espelhado em uma configuração MetroCluster .

- **Cargas de trabalho definidas pelo sistema**

Os processos internos envolvidos com eficiência de armazenamento, replicação de dados e integridade do sistema, incluindo:

- Eficiência de armazenamento, como desduplicação
- Saúde do disco, que inclui reconstrução de RAID, limpeza de disco e assim por diante
- Replicação de dados, como cópias do SnapMirror
- Atividades de gestão
- Saúde do sistema de arquivos, que inclui várias atividades WAFL
- Scanners de sistema de arquivos, como o WAFL scan
- Descarregamento de cópia, como operações de eficiência de armazenamento descarregadas de hosts VMware
- Saúde do sistema, como movimentações de volume, compactação de dados e assim por diante
- Volumes não monitorados

Os dados de desempenho para cargas de trabalho definidas pelo sistema são exibidos na GUI somente quando o componente do cluster usado por essas cargas de trabalho está em contenção. Por exemplo, você não pode pesquisar o nome de uma carga de trabalho definida pelo sistema para visualizar seus dados de desempenho na GUI.

Valores de medição de desempenho da carga de trabalho

O Unified Manager mede o desempenho das cargas de trabalho em um cluster com base em valores estatísticos históricos e esperados, que formam a previsão de latência dos valores para as cargas de trabalho. Ele compara os valores estatísticos reais da carga de trabalho com a previsão de latência para determinar quando o desempenho da carga de trabalho está muito alto ou muito baixo. Uma carga de trabalho que não está funcionando conforme o esperado aciona um evento de desempenho dinâmico para notificá-lo.

Na ilustração a seguir, o valor real, em vermelho, representa as estatísticas de desempenho reais no período. O valor real ultrapassou o limite de desempenho, que é o limite superior da previsão de latência. O pico é o maior valor real 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	A porcentagem do limite de QoS usado pelas cargas de trabalho no grupo de políticas. i Se o Unified Manager detectar uma alteração em um grupo de políticas, como adicionar ou remover um volume ou alterar o limite de QoS, os valores reais e esperados poderão exceder 100% do limite definido. Se um valor exceder 100% do limite definido, ele será exibido como >100%. Se um valor for menor que 1% do limite definido, ele será exibido como <1%.
Real	O valor de desempenho medido em um momento específico para uma determinada carga de trabalho.
Desvio	A mudança entre os valores esperados e os valores reais. É a razão entre o valor real menos o valor esperado e o valor superior do intervalo esperado menos o valor esperado. i Um valor de desvio negativo indica que o desempenho da carga de trabalho é menor que o esperado, enquanto um valor de desvio positivo indica que o desempenho da carga de trabalho é maior que o esperado.

Medição	Descrição
Esperado	Os valores esperados são baseados na análise de dados históricos de desempenho 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 de quais são os valores máximos e mínimos de desempenho esperados em um momento específico. Para a latência da carga de trabalho, os valores superiores formam o limite de desempenho. Quando o valor real ultrapassa o limite de desempenho, o Unified Manager aciona um evento de desempenho dinâmico.
Pico	O valor máximo medido ao longo de um período de tempo.
Desvio de pico	O valor máximo de desvio medido ao longo de 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, processamento de dados e agregados, a porcentagem de tempo ocupado para concluir as operações de carga de trabalho ao longo de um período de tempo. Por exemplo, a porcentagem de tempo para os componentes de processamento de rede ou de dados 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), de cargas de trabalho em um cluster local para o cluster parceiro em uma configuração MetroCluster .

Qual é a faixa de desempenho esperada

A previsão de latência é uma previsão de quais são os valores máximos e mínimos de desempenho esperados em um momento específico. Para a latência da carga de trabalho, os valores superiores formam o limite de desempenho. Quando o valor real ultrapassa o limite de desempenho, o Unified Manager aciona um evento de desempenho dinâmico.

Por exemplo, durante o horário comercial normal, entre 9h e 17h, a maioria dos funcionários pode verificar

seus e-mails entre 9h e 10h30. 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 o horário de almoço, entre 12h e 13h, e no final do dia de trabalho, após as 17h, a maioria dos funcionários provavelmente está longe de seus computadores. A demanda nos servidores de e-mail normalmente diminui, diminuindo também 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 depois das 17h e aumentam a atividade no armazenamento de back-end.

Ao longo de vários dias, o aumento e a diminuição na atividade da carga de trabalho 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 de um objeto está fora dos limites superiores ou inferiores e permanece fora dos limites por um período de tempo, isso pode indicar que o objeto está sendo usado em excesso ou em falta.

Como a previsão de latência é formada

O Unified Manager deve coletar no mínimo 3 dias de atividade de carga de trabalho antes de poder iniciar sua análise e antes que a previsão de latência para o tempo de resposta de E/S possa ser exibida na GUI. A coleta mínima de dados necessária não leva em conta todas as mudanças 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 00:00 para refletir as alterações na atividade da carga de trabalho e estabelecer um limite de desempenho 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, o que leva aproximadamente 15 dias para ser concluído. Durante esse período, você pode continuar a usar o Unified Manager, mas, como o Unified Manager usa a previsão de latência para detectar eventos dinâmicos, alguns eventos podem não ser precisos. Eventos detectados antes da mudança de horário 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) para suas cargas de trabalho monitoradas. Ele alerta você quando a latência real de uma carga de trabalho está acima dos limites superiores da previsão de latência, o que aciona um evento de desempenho dinâmico, para que você possa analisar o problema de desempenho 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 o desempenho esperado e os níveis de atividade 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 do intervalo esperado. A comparação entre os valores reais e os valores esperados cria um perfil de desempenho para a carga de trabalho.

Quando a latência real de uma carga de trabalho excede o limite de desempenho dinâmico, devido à contenção em um componente do cluster, a latência é alta e a carga de trabalho tem um desempenho mais lento do que o esperado. O desempenho de outras cargas de trabalho que compartilham os mesmos componentes do cluster também pode ser mais lento do que o esperado.

O Unified Manager analisa o evento de ultrapassagem de limite e determina se a atividade é um evento de desempenho. Se a alta atividade de carga de trabalho 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 de desempenho dinâmico.

Algumas cargas de trabalho podem ter atividade consistentemente baixa, onde a previsão de latência não tem uma alta taxa de mudança ao longo do tempo. Para minimizar o número de eventos durante a análise de eventos de desempenho, o Unified Manager aciona um evento somente 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 seu valor mais baixo e 5,5 ms/op no seu valor mais alto. 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 do cluster, ela estará acima da previsão de latência e terá excedido o limite de desempenho dinâmico.

Quando o tráfego de rede diminui ou o componente do cluster não está mais em disputa, 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 da carga de trabalho para identificar problemas de desempenho

A latência da carga de trabalho (tempo de resposta) é o tempo que um volume em um cluster leva para responder a solicitações de E/S de aplicativos clientes. O Unified Manager usa a latência para detectar e alertá-lo sobre eventos de desempenho.

Uma latência alta significa que as solicitações de aplicativos para um volume em um cluster estão demorando mais 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 externos ao cluster, como gargalos de rede, problemas com o cliente que hospeda os aplicativos ou problemas com os próprios aplicativos.

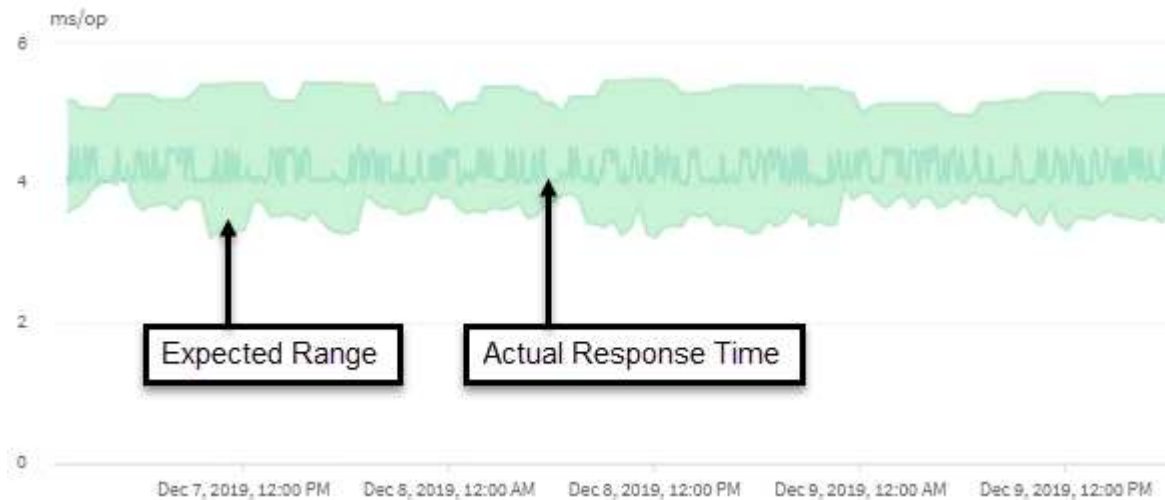


O Unified Manager monitora apenas a atividade da carga de trabalho no cluster. Ele não monitora os aplicativos, os clientes ou os caminhos entre os aplicativos e o cluster.

Operações no cluster, como fazer backups ou executar desduplicação, que aumentam a demanda de componentes do cluster compartilhados por outras cargas de trabalho também podem contribuir para alta

latência. Se a latência real exceder o limite de desempenho dinâmico do intervalo esperado (previsão de latência), o Unified Manager analisará o evento para determinar se é um evento de desempenho que você pode precisar resolver. A latência é medida em milissegundos por operação (ms/op).

No gráfico Latência Total na página Análise de Carga de Trabalho, você pode 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 gerais de latência. A comparação ajuda a determinar quais operações têm a maior atividade 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 da carga de trabalho ou os componentes do cluster que estão envolvidos no evento.



Este exemplo mostra o gráfico de latência. A atividade real de tempo de resposta (latência) é uma linha azul e a previsão de latência (intervalo esperado) é verde.

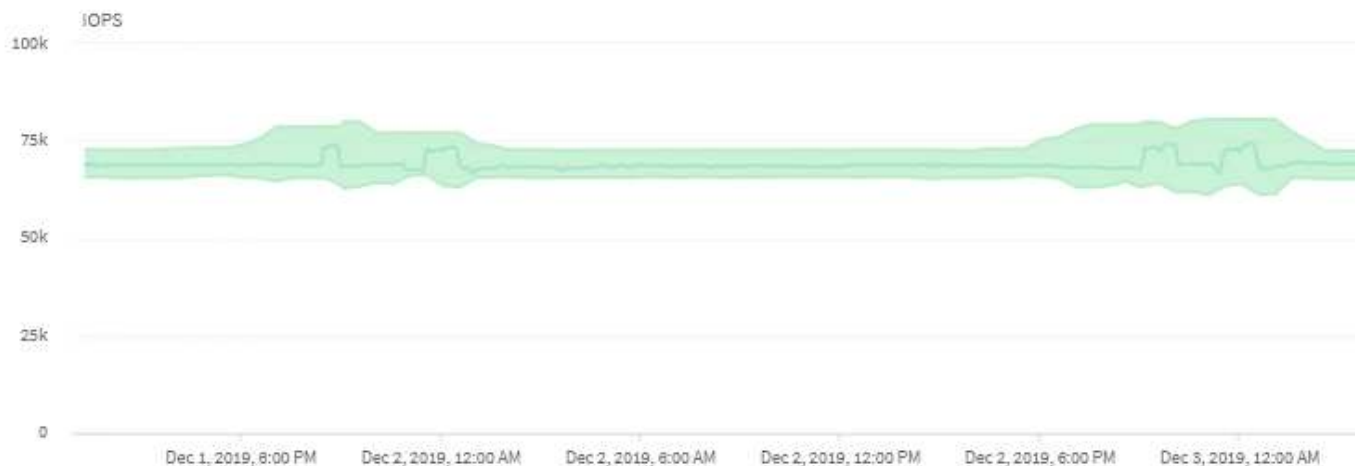


Pode haver lacunas na linha azul se o Unified Manager não conseguir coletar dados. Isso pode ocorrer porque o cluster ou volume estava inacessível, o Unified Manager estava desativado durante esse período ou a coleta estava demorando mais do que o período de coleta de 5 minutos.

Como as operações de cluster podem afetar a latência da carga de trabalho

Operações (IOPS) representam a atividade de todas as cargas de trabalho definidas pelo usuário e pelo sistema em um cluster. As estatísticas de IOPS ajudam a determinar se os processos de cluster, como fazer backups ou executar deduplicação, estão afetando a latência da carga de trabalho (tempo de resposta) ou podem ter causado ou contribuído para um evento de desempenho.

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 da carga de trabalho que podem ter sido os principais contribuintes para o evento de desempenho. IOPS são medidos em operações por segundo (ops/seg).



Este exemplo mostra o gráfico IOPS. As estatísticas operacionais reais são uma linha azul e a previsão do IOPS das estatísticas operacionais 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 o Unified Manager analisar. Você precisa reduzir os recursos que o cluster está usando para que as estatísticas possam ser coletadas.

Monitoramento de desempenho das configurações do MetroCluster

O Unified Manager permite monitorar a taxa de transferência de gravação entre clusters em uma configuração MetroCluster para identificar cargas de trabalho com alta taxa de transferência de gravação.

Se essas cargas de trabalho de alto desempenho estiverem fazendo com que outros volumes no cluster local tenham altos tempos de resposta de E/S, o Unified Manager acionará eventos de desempenho para notificá-lo.



O Unified Manager trata os clusters em uma configuração MetroCluster como clusters individuais. Ele não distingue entre clusters que são parceiros nem correlaciona a taxa de transferência de gravação de cada cluster.

Quando um cluster local em uma configuração MetroCluster espelha seus dados para seu cluster parceiro, os dados são gravados na NVRAM e então transferidos pelos links entre switches (ISLs) para os agregados remotos. O Unified Manager analisa a NVRAM para identificar as cargas de trabalho cujo alto rendimento de gravação está utilizando excessivamente a NVRAM, colocando NVRAM em contenção.

Cargas de trabalho cujo desvio no tempo de resposta excedeu o limite de desempenho são chamadas de *vítimas* e cargas de trabalho cujo desvio na taxa de transferência de gravação para a NVRAM é maior que o normal, causando a contenção, são chamadas de *valentões*. Como somente as solicitações de gravação são espelhadas no cluster do parceiro, o Unified Manager não analisa a taxa de transferência de leitura.

Você pode visualizar a taxa de transferência de qualquer um dos clusters em uma configuração do MetroCluster analisando as cargas de trabalho dos LUNs e volumes correspondentes nas telas a seguir. Você pode filtrar os resultados por cluster. No painel de navegação esquerdo:

- **Armazenamento > Clusters > Desempenho: visualização Todos os clusters.** Ver
- **Armazenamento > Volumes > Desempenho: visualização Todos os volumes.**
- **Armazenamento > LUNs > Desempenho: visualização de todos os LUNs.**
- **Análise de carga de trabalho > Todas as cargas de trabalho**

Informações relacionadas

["Análise e notificação de eventos de desempenho"](#)

["Análise de eventos de desempenho para uma configuração do MetroCluster"](#)

["Funções das cargas de trabalho envolvidas em um evento de desempenho"](#)

["Identificação das cargas de trabalho das vítimas envolvidas em um evento de desempenho"](#)

["Identificando cargas de trabalho agressivas envolvidas em um evento de desempenho"](#)

["Identificação de cargas de trabalho de tubarão envolvidas em um evento de desempenho"](#)

Entenda eventos de desempenho e alertas

Eventos de desempenho são incidentes relacionados ao desempenho da carga de trabalho em um cluster. Eles ajudam você a identificar cargas de trabalho com tempos de resposta lentos. Juntamente com os 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 desempenho são problemas relacionados ao desempenho da carga de trabalho em um cluster. Eles ajudam você a identificar objetos de armazenamento 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 com base em valores de limite personalizados que você definiu. Você configura políticas de limite de desempenho para objetos de armazenamento; por exemplo, agregados e volumes, para que eventos sejam gerados quando um valor limite para um contador de desempenho for violado.

Você deve definir uma política de limite de desempenho e atribuí-la a um objeto de armazenamento para

receber esses eventos.

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

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

Essas políticas de limite são ativadas por padrão, e você poderá ver eventos logo após adicionar um cluster.

- **Eventos de limite de desempenho dinâmico**

Problemas de desempenho que são resultado de falhas ou erros em uma infraestrutura de TI ou de cargas de trabalho que utilizam excessivamente os recursos do cluster. A causa desses eventos pode ser um problema simples que se corrige sozinho ao longo do 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 alto uso de componentes de cluster compartilhados.

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

Tipos de gravidade de eventos de desempenho

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

- **Crítico**

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

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

- **Aviso**

Um contador de desempenho para um objeto de cluster está fora da faixa normal e deve ser monitorado para garantir que não atinja a gravidade crítica. Eventos dessa gravidade não causam interrupção do serviço e pode não ser necessária ação corretiva imediata.

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 alguma alteração de configuração, o evento com tipo de gravidade Informação é gerado.

Eventos de informação são enviados diretamente do ONTAP quando ele detecta uma alteração de configuração.

Para mais informações, consulte os seguintes links:

- "O que acontece quando um evento é recebido"
- "Quais informações estão contidas em um e-mail de alerta"
- "Adicionando alertas"
- "Adicionar alertas para eventos de desempenho"

Alterações de configuração detectadas pelo Unified Manager

O Unified Manager monitora seus clusters em busca de alterações de configuração para ajudar você a determinar se uma alteração pode ter causado ou contribuído para um evento de desempenho. As páginas do Performance Explorer exibem um ícone de evento de alteração () para indicar a data e a hora em que a alteração foi detectada.

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 alteração impactou o desempenho do objeto de cluster selecionado. Se a alteração foi detectada no mesmo momento ou próximo a um evento de desempenho, a alteração pode ter contribuído para o problema, o que fez com que o alerta do evento fosse acionado.

O Unified Manager pode detectar os seguintes eventos de alteração, que são categorizados como eventos informativos:

- Um volume se move entre agregados.

O Unified Manager pode detectar quando a movimentação está em andamento, concluída ou falhou. Se o Unified Manager estiver inativo durante uma movimentação de volume, quando ele voltar a funcionar, ele detectará a movimentação de volume e exibirá um evento de alteração para ela.

- O limite de taxa de transferência (MB/s ou IOPS) de um grupo de políticas de QoS que contém uma ou mais cargas de trabalho monitoradas muda.

Alterar um limite de 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 retorna gradualmente ao normal e quaisquer eventos causados pelos picos se tornam obsoletos.

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

O Unified Manager pode detectar quando a operação de aquisição, aquisição parcial ou devolução foi concluída. Se a aquisição for causada por um nó em pânico, o Unified Manager não detectará o evento.

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

A versão anterior e a nova versão são exibidas.

Tipos de políticas de limite de desempenho 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 informação quando os limites de desempenho monitorados são violados.



As políticas de limite de desempenho definidas pelo sistema não estão habilitadas nos sistemas Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select .

Se estiver recebendo eventos desnecessários de quaisquer políticas de limite de desempenho definidas pelo sistema, você poderá desabilitar os eventos para políticas individuais na página Configuração de Eventos.

Políticas de limite de cluster

As políticas de limite de desempenho do cluster definidas pelo sistema são atribuídas, por padrão, a cada cluster monitorado pelo Unified Manager:

- **Desequilíbrio de carga do 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 da carga de trabalho.

Ele faz isso comparando o valor da capacidade de desempenho usada para todos os nós em um cluster para ver se algum nó excedeu o valor limite de 30% por mais de 24 horas. Este é um evento de alerta.

- **Desequilíbrio de capacidade do cluster**

Identifica situações em que um agregado tem uma capacidade utilizada muito maior do que outros agregados no cluster e, portanto, pode afetar o espaço necessário para as operações.

Ele faz isso comparando o valor da capacidade usada para todos os agregados no cluster para ver se há uma diferença de 70% entre quaisquer agregados. Este é um evento de alerta.

Políticas de limite de nó

As políticas de limite de desempenho de nó definidas pelo sistema são atribuídas, por padrão, a cada nó nos clusters monitorados pelo Unified Manager:

- **Limite de capacidade de desempenho utilizada ultrapassado**

Identifica situações em que um único nó está operando acima dos limites de sua eficiência operacional e, portanto, potencialmente afetando as latências da carga de trabalho.

Ele faz isso procurando por nós que estão usando mais de 100% de sua capacidade de desempenho por mais de 12 horas. Este é um evento de alerta.

- **Par de nós HA superutilizado**

Identifica situações em que os nós em um par HA estão operando acima dos limites de eficiência operacional do par HA.

Ele faz isso observando o valor da capacidade de desempenho usada para os dois nós no par HA. Se a capacidade de desempenho combinada usada pelos dois nós exceder 200% por mais de 12 horas, um failover do controlador afetará as latências da carga de trabalho. Este é um evento informativo.

- **Fragmentação do disco do nó**

Identifica situações em que um disco ou discos em um agregado são fragmentados, tornando lentos os principais serviços do sistema e potencialmente afetando as latências da carga de trabalho em um nó.

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



A política “Fragmentação de disco de nó” analisa agregados somente de HDD; agregados de Flash Pool, SSD e FabricPool não são analisados.

Políticas de limite agregado

A política de limite de desempenho agregado definida pelo sistema é atribuída por padrão a cada agregado nos clusters monitorados pelo Unified Manager:

• Discos agregados superutilizados

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

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

Algumas das atividades de manutenção em segundo plano pelas quais um disco pode estar passando são reconstrução de disco, limpeza de disco, ressincronização do SyncMirror e reparação.

- Há um gargalo de comunicação na interconexão Fibre Channel da prateleira de disco?
- Há pouco espaço livre no agregado? Um evento de aviso é emitido para esta política somente 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 utilizados em mais de 95%.



A política “Discos agregados superutilizados” analisa agregados somente de HDD e agregados de Flash Pool (híbridos); agregados de SSD e FabricPool não são analisados.

Políticas de limite de latência de carga de trabalho

As políticas de limite de latência de carga de trabalho definidas pelo sistema são atribuídas a qualquer carga de trabalho que tenha uma política de Nível de Serviço de Desempenho configurada com um valor de “latência esperada” definido:

• Limite de latência de LUN/volume de carga de trabalho violado, conforme definido pelo nível de serviço de desempenho

Identifica volumes (compartilhamentos de arquivos) e LUNs que excederam seu limite de “latência esperada” e que estão afetando o desempenho da carga de trabalho. Este é um evento de alerta.

Ele faz isso procurando por cargas de trabalho que excederam o valor de latência esperado em 30% do tempo durante a hora anterior.

Políticas de limite de QoS

As políticas de limite de desempenho de QoS definidas pelo sistema são atribuídas a qualquer carga de trabalho 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 da carga de trabalho é 15% menor que o valor de QoS configurado:

- **Limite máximo de QoS IOPS ou MB/s**

Identifica volumes e LUNs que excederam seu limite máximo de IOPS ou MB/s de taxa de transferência de QoS e que estão afetando a latência da carga de trabalho. Este é um evento de alerta.

Quando uma única carga de trabalho é atribuída a um grupo de políticas, isso é feito procurando por cargas de trabalho que excederam o limite máximo de taxa de transferência definido no grupo de políticas de QoS atribuído durante cada período de coleta da hora anterior.

Quando várias cargas de trabalho compartilham uma única política de QoS, isso é feito adicionando o IOPS ou MB/s de todas as cargas de trabalho na política e verificando esse total em relação ao limite.

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

Identifica volumes que excederam seu limite de taxa de transferência de pico de IOPS/TB de QoS adaptável (ou IOPS/TB com limite de tamanho de bloco) e que estão afetando a latência da carga de trabalho. Este é um evento de alerta.

Ele faz isso convertendo o limite de pico 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, procura volumes que excederam o IOPS máximo de QoS durante cada período de coleta de desempenho da hora anterior.



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

Quando o elemento “tamanho do bloco” é definido na política de QoS adaptável, o limite é convertido em um valor máximo de QoS em MB/s com base no tamanho de cada volume. Em seguida, ele procura volumes que excederam o QoS máximo de MB/s durante cada período de coleta de desempenho da hora anterior.



Esta 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 desempenho

Eventos de desempenho notificam você sobre problemas de desempenho de E/S em uma carga de trabalho causados por contenção em um componente do cluster. O Unified Manager analisa o evento para identificar todas as cargas de trabalho envolvidas, o componente em contenção e se o evento ainda é um problema que você precisa resolver.

O Unified Manager monitora a latência de E/S (tempo de resposta) e IOPS (operações) para volumes em um cluster. Quando outras cargas de trabalho usam excessivamente um componente do cluster, por exemplo, o componente fica em contenção e não consegue ter um desempenho ideal para atender às demandas da carga de trabalho. O desempenho de outras cargas de trabalho que usam o mesmo componente pode ser afetado, causando aumento de latência. 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 executa as seguintes análises, usando os 15 dias anteriores de estatísticas de desempenho, para identificar as cargas de trabalho das vítimas, as cargas de trabalho dos agressores e o

componente do cluster envolvido em um evento:

- Identifica cargas de trabalho de vítimas cuja latência ultrapassou o limite de desempenho dinâmico, que é o limite superior da previsão de latência:
 - Para volumes em agregados híbridos de HDD ou Flash Pool (camada local), os eventos são acionados somente quando a latência é maior que 5 milissegundos (ms) e o IOPS é maior que 10 operações por segundo (ops/seg).
 - Para volumes em agregados totalmente SSD ou agregados FabricPool (camada de nuvem), os eventos são acionados somente quando a latência é maior que 1 ms e o IOPS é maior que 100 ops/s.
- Identifica o componente do cluster em contenção.



Se a latência das cargas de trabalho das vítimas na interconexão do cluster for maior que 1 ms, o Unified Manager tratará isso como significativo e acionará um evento para a interconexão do cluster.

- Identifica as cargas de trabalho agressivas que estão usando excessivamente o componente do cluster e fazendo com que ele fique em contenção.
- Classifica as cargas de trabalho envolvidas, com base no desvio na utilização ou atividade de um componente do cluster, para determinar quais agressores têm a maior alteração no uso do componente do cluster e quais vítimas são as mais impactadas.

Um evento pode ocorrer apenas por um breve momento e depois se corrigir depois que o componente que ele está usando não estiver 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, cluster e componentes de cluster envolvidos.



Um único volume pode estar 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 reconhecido). O problema que causou o evento não foi corrigido ou não foi resolvido. O contador de desempenho do objeto de armazenamento permanece acima do limite de desempenho.

• Obsoleto

Indica que o evento não está mais ativo. O problema que causou o evento foi corrigido ou resolvido. O contador de desempenho do objeto de armazenamento 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 alertas para esses eventos são enviados para endereços de e-mail especificados. Você pode visualizar informações

detalhadas de análise sobre um evento e obter sugestões para resolvê-lo na página 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 no 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 disputa é circulado e destacado em vermelho. Você pode clicar em **Ver análise completa** para ver a análise completa na página de detalhes do evento. Se houver vários eventos no mesmo período, a caixa de diálogo mostrará detalhes sobre os três eventos mais recentes. Você pode clicar em um evento para visualizar a análise do evento na página 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) de uma carga de trabalho para determinar o nível de impacto no desempenho da carga de trabalho. Essas informações determinam a função de cada carga de trabalho no evento e como elas são classificadas na página 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 últimos valores analisados 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 a Carga de Trabalho A é de 5 a 10 milissegundos por operação (ms/op) e sua latência real geralmente é em torno de 7 ms/op. A previsão de latência para a Carga de Trabalho B é de 10 a 20 ms/op e sua latência real geralmente é em torno de 15 ms/op. Ambas as cargas de trabalho estão 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 o limite superior da previsão de latência, e acionando eventos. O desvio na 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 a Carga de Trabalho B é de cerca de 25 ms/op. A latência de ambas as cargas de trabalho atingiu o pico de 40 ms/op, mas a carga de trabalho A teve o maior impacto no desempenho porque teve o maior desvio de latência em 33 ms/op.

Na página Detalhes do evento, na seção Diagnóstico do sistema, você pode classificar as cargas de trabalho por desvio em atividade, utilização ou taxa de transferência para um componente do cluster. Você também pode classificar cargas de trabalho 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 em relação aos valores esperados para determinar a ordem de classificação da carga de trabalho. Para a latência, os pontos vermelhos (●) indicam um limite de desempenho ultrapassado por uma carga de trabalho da vítima e o impacto subsequente na latência. Cada ponto vermelho indica um nível maior de desvio na latência, o que ajuda a identificar as cargas de trabalho das vítimas cuja latência foi mais impactada por um

evento.

Componentes do cluster e por que eles podem estar em disputa

Você pode identificar problemas de desempenho do cluster quando um componente do cluster entra em contenção. O desempenho das cargas de trabalho que usam o componente fica lento 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 ter um desempenho ideal. Seu desempenho diminuiu, e o desempenho de outros componentes do cluster e cargas de trabalho, chamados de *vítimas*, podem ter aumentado a latência. Para tirar um componente da disputa, você deve reduzir sua carga de trabalho ou aumentar sua capacidade de lidar com mais trabalho, para que o desempenho possa retornar aos níveis normais. Como o Unified Manager coleta e analisa o desempenho da carga de trabalho em intervalos de cinco minutos, ele detecta apenas quando um componente do cluster é usado em excesso de forma consistente. Picos transitórios de uso excessivo que duram apenas um curto período dentro do intervalo de cinco minutos não são detectados.

Por exemplo, um agregado de armazenamento pode estar em disputa porque uma ou mais cargas de trabalho nele estão competindo para que suas solicitações de E/S sejam atendidas. Outras cargas de trabalho no agregado podem ser impactadas, causando diminuição de desempenho. Para reduzir a quantidade de atividade no agregado, há diferentes etapas que você pode seguir, como mover uma ou mais cargas de trabalho para um agregado ou nó menos ocupado, para diminuir a demanda geral de carga de trabalho no agregado atual. Para um grupo de políticas de QoS, você pode ajustar o limite de taxa de transferência ou mover cargas de trabalho para um grupo de políticas diferente, para que as cargas de trabalho não sejam mais limitadas.

O Unified Manager monitora os seguintes componentes do cluster para alertá-lo quando eles estão em contenção:

- **Rede**

Representa o tempo de espera de solicitações de E/S pelos protocolos de rede externos no cluster. O tempo de espera é o tempo gasto esperando que as transações “transferência pronta” 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 afetando 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 nó que manipula o processamento da rede pode ter mudado 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 afetando a latência de uma ou mais cargas de trabalho.

Ao usar um cluster All SAN Array em uma configuração ativa-ativa, o valor de latência de processamento da rede é exibido para ambos os nós para que você possa verificar se os nós estão compartilhando a carga igualmente.

- **Limite Máximo de QoS**

Representa a configuração máxima (pico) de taxa de transferência do grupo de políticas de Qualidade de Serviço (QoS) de armazenamento atribuído à carga de trabalho. Se o componente do grupo de políticas

estiver em contenção, isso significa que todas as cargas de trabalho no grupo de políticas estão sendo limitadas pelo limite de taxa de transferência definido, o que está impactando a latência de uma ou mais dessas cargas de trabalho.

- **Limite mínimo de QoS**

Representa a latência para uma carga de trabalho que está sendo causada pela configuração mínima (esperada) de taxa de transferência de QoS atribuída a outras cargas de trabalho. Se o QoS mínimo definido em determinadas cargas de trabalho usar a maior parte da largura de banda para garantir a taxa de transferência prometida, outras cargas de trabalho serão limitadas e terão mais latência.

- **Interconexão de Cluster**

Representa os cabos e adaptadores com os quais os nós agrupados estão fisicamente conectados. Se o componente de interconexão do cluster estiver em contenção, isso significa que o alto tempo de espera para solicitações de E/S na interconexão do cluster está afetando a latência de uma ou mais cargas de trabalho.

- *** Data Processing***

Representa o componente de software no cluster envolvido com o processamento de E/S entre o cluster e o agregado de armazenamento que contém a carga de trabalho. O nó que manipula o processamento de dados pode ter mudado desde que o evento foi detectado. Se o componente de processamento de dados estiver em contenção, isso significa que a alta utilização no nó de processamento de dados está afetando a latência de uma ou mais cargas de trabalho.

- **Ativação de Volume**

Representa o processo que rastreia o uso de todos os volumes ativos. Em ambientes grandes onde mais de 1000 volumes estão ativos, esse processo rastreia quantos volumes críticos precisam acessar recursos por meio do nó ao mesmo tempo. Quando o número de volumes ativos simultâneos excede o limite máximo recomendado, alguns dos volumes não críticos sofrerão latência, conforme identificado aqui.

- *** Recursos do MetroCluster ***

Representa os recursos do MetroCluster , incluindo NVRAM e links entre switches (ISLs), usados para espelhar dados entre clusters em uma configuração do MetroCluster . Se o componente MetroCluster estiver em contenção, isso significa que há alta taxa de transferência de gravação de cargas de trabalho no cluster local ou um problema de integridade do link que está afetando a latência de uma ou mais cargas de trabalho no cluster local. Se o cluster não estiver em uma configuração MetroCluster , este ícone não será exibido.

- **Operações agregadas ou SSD agregadas**

Representa o agregado de armazenamento no qual as cargas de trabalho estão sendo executadas. Se o componente agregado estiver em contenção, isso significa que a alta utilização no agregado está afetando a latência de uma ou mais cargas de trabalho. Um agregado consiste em todos os HDDs ou uma mistura de HDDs e SSDs (um agregado Flash Pool) ou uma mistura de HDDs e uma camada de nuvem (um agregado FabricPool). Um “Agregado SSD” consiste em todos os SSDs (um agregado all-flash) ou uma mistura de SSDs e uma camada de nuvem (um 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 estão impactando a latência de uma ou mais cargas de trabalho.

- **Sincronizar SnapMirror**

Representa o componente de software no cluster envolvido na replicação de dados do usuário do volume primário para o volume secundário em um relacionamento síncrono do SnapMirror . Se o componente de sincronização SnapMirror estiver em contenção, isso significa que a atividade das operações síncronas do SnapMirror está impactando a latência de uma ou mais cargas de trabalho.

Funções das cargas de trabalho envolvidas em um evento de desempenho

O Unified Manager usa funções para identificar o envolvimento de uma carga de trabalho em um evento de desempenho. Os papéis incluem vítimas, valentões e tubarões. Uma carga de trabalho definida pelo usuário pode ser uma vítima, um agressor e um tubarão ao mesmo tempo.

Papel	Descrição
Vítima	Uma carga de trabalho definida pelo usuário cujo desempenho diminuiu devido a outras cargas de trabalho, chamadas de bullies, que estão usando excessivamente um componente do cluster. Somente cargas de trabalho definidas pelo usuário são identificadas como vítimas. O Unified Manager identifica as cargas de trabalho das vítimas com base no desvio de latência, onde a latência real, durante um evento, aumentou muito em relação à previsão de latência (intervalo esperado).
Valentão	Uma carga de trabalho definida pelo usuário ou pelo sistema cujo uso excessivo de um componente do cluster fez com que o desempenho de outras cargas de trabalho, chamadas vítimas, diminuísse. O Unified Manager identifica cargas de trabalho agressivas com base no desvio no uso de um componente do cluster, onde o uso real, durante um evento, aumentou muito em relação ao intervalo de uso esperado.
Tubarão	Uma carga de trabalho definida pelo usuário com o maior uso de um componente de cluster em comparação com todas as cargas de trabalho envolvidas em um evento. O Unified Manager identifica cargas de trabalho tubarões com base no uso de um componente de cluster durante um evento.

As cargas de trabalho em um cluster podem compartilhar muitos dos componentes do cluster, como agregados e a CPU para processamento de rede e dados. Quando uma carga de trabalho, como um volume, aumenta o uso de um componente de cluster a ponto de o componente não conseguir atender às demandas de carga de trabalho com eficiência, o componente está em contenção. A carga de trabalho que utiliza excessivamente um componente do cluster é um problema. As outras cargas de trabalho que compartilham esses componentes e cujo desempenho é afetado pelo agressor são as vítimas. Atividades de cargas de

trabalho definidas pelo sistema, como desduplicação ou cópias de instantâneos, também podem evoluir para "bullying".

Quando o Unified Manager detecta um evento, ele identifica todas as cargas de trabalho e componentes de cluster envolvidos, incluindo as cargas de trabalho agressivas que causaram o evento, o componente de cluster que está em contenção e as cargas de trabalho vítimas cujo desempenho diminuiu devido ao aumento da atividade das cargas de trabalho agressivas.



Se o Unified Manager não conseguir identificar as cargas de trabalho agressivas, ele alertará apenas sobre as cargas de trabalho das vítimas e o componente do cluster envolvido.

O Unified Manager pode identificar cargas de trabalho que são vítimas de cargas de trabalho de intimidação e também identificar quando essas mesmas cargas de trabalho se tornam cargas de trabalho de intimidação. Uma carga de trabalho pode ser um agressor para si mesma. Por exemplo, uma carga de trabalho de alto desempenho que está sendo limitada por um limite de grupo de políticas faz com que todas as cargas de trabalho no grupo de políticas sejam limitadas, incluindo ela mesma. Uma carga de trabalho que é um agressor ou uma vítima em um evento de desempenho em andamento pode mudar sua função ou não ser mais um participante do evento.

Gerenciar limites de desempenho

As políticas de limite de desempenho permitem que você determine o ponto em que o Unified Manager gera um evento para informar os administradores do sistema sobre problemas que podem estar afetando o desempenho da carga de trabalho. Essas políticas de limite são conhecidas como limites de desempenho *definidos pelo usuário*.

Esta versão oferece suporte a limites de desempenho dinâmicos, definidos pelo usuário e pelo sistema. Com limites de desempenho dinâmicos e definidos pelo sistema, o Unified Manager analisa a atividade da carga de trabalho para determinar o valor limite apropriado. Com limites definidos pelo usuário, você pode definir os limites superiores de desempenho para muitos contadores de desempenho e para muitos objetos de armazenamento.



Os limites de desempenho definidos pelo sistema e os limites de desempenho dinâmico são definidos pelo Unified Manager e não são configuráveis. Se estiver recebendo eventos desnecessários de quaisquer políticas de limite de desempenho definidas pelo sistema, você pode desabilitar políticas individuais na página Configuração de Eventos.

Como funcionam as políticas de limite de desempenho definidas pelo usuário

Defina políticas de limite de desempenho em objetos de armazenamento (por exemplo, em agregados e volumes) para que um evento possa ser enviado ao administrador de armazenamento para informá-lo de que o cluster está enfrentando um problema de desempenho.

Você cria uma política de limite de desempenho para um objeto de armazenamento por meio de:

- Selecionando um objeto de armazenamento
- Selecionando um contador de desempenho associado a esse objeto
- Especificar valores que definem os limites superiores do contador de desempenho que são considerados situações de advertência e críticas

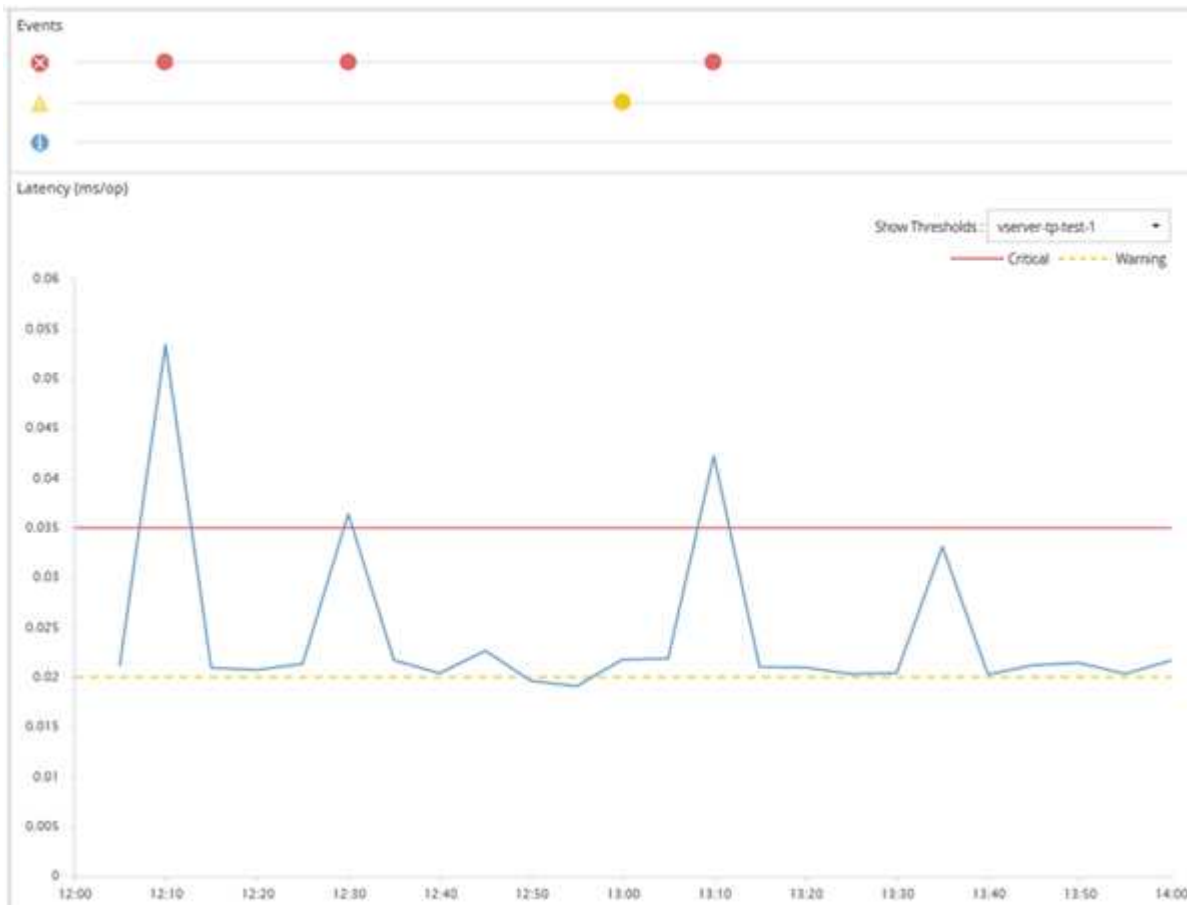
- Especificando um período de tempo que define por quanto tempo o contador deve exceder o limite superior

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 durante 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 durante 10 minutos.



A versão atual fornece limites que enviam eventos quando um valor de contador excede a configuração de limite. Não é possível definir limites que enviem eventos quando um valor do contador cair abaixo de uma configuração de limite.

Um exemplo de gráfico de contador é mostrado aqui, indicando que um limite de alerta (ícone amarelo) foi violado às 13h00 e que um limite crítico (ícone vermelho) foi violado às 12h10, 12h30 e 13h10:



Uma violação de limite deve ocorrer continuamente durante o período especificado. Se o limite cair abaixo dos valores-limite por qualquer motivo, uma violação subsequente será considerada o início de uma nova duração.

Alguns objetos de cluster e contadores de desempenho permitem que você crie 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 alerta	Limiar crítico	Duração
Volume	Latência	10 milissegundos	20 milissegundos	15 minutos

Objeto de cluster	Contador de desempenho	Limite de alerta	Limiar crítico	Duração
Agregar	Utilização	65%	85%	

Políticas de limite que usam dois objetos de cluster fazem com que um evento seja gerado somente quando ambas as condições são 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 relatado.
15 milissegundos	75%	Um evento de Aviso é relatado.
25 milissegundos	75%	Um evento de Aviso é relatado.
25 milissegundos	90%	Um evento crítico é relatado.

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, na página Resumo do Cluster de Desempenho, na página Eventos e na página Inventário de Desempenho específica do objeto.
- (opcional) Um alerta por e-mail sobre o evento pode ser enviado a um ou mais destinatários de e-mail, e uma interceptação SNMP pode ser enviada a um receptor de interceptação.
- (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 limite de Aviso ou Crítico for violada.

Após uma violação de política de limite de desempenho ocorrer em um objeto de armazenamento, nenhum outro evento será gerado para essa política até que o valor do contador fique abaixo do valor limite, momento em que a duração é redefinida para esse limite. Enquanto o limite continua sendo excedido, o horário de término do evento é continuamente atualizado para refletir que o evento está em andamento.

Um evento de limite captura ou congela as informações relacionadas à gravidade e à definição da política para que 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. Há outros contadores que podem ter limites definidos apenas para determinados objetos de armazenamento.

Contadores de desempenho disponíveis

Objeto de armazenamento	Contador de desempenho	Descrição
Conjunto	IOPS	Número médio de operações de entrada/saída que o cluster processa por segundo.
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 do aplicativo.
Utilização	Porcentagem média da CPU e da RAM do nó que está sendo usada.	Capacidade de Desempenho Utilizada
Porcentagem média de capacidade de desempenho que está sendo consumida pelo nó.	Capacidade de Desempenho Utilizada - Aquisição	Porcentagem média da capacidade de desempenho que está sendo consumida pelo nó, mais a capacidade de desempenho do nó parceiro.
Agregar	IOPS	Número médio de operações de entrada/saída processadas pelo agregado 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 de discos do agregado que estão sendo utilizados.
Capacidade de Desempenho Utilizada	Porcentagem média da capacidade de desempenho que está sendo consumida pelo agregado.	VM de armazenamento

Objeto de armazenamento	Contador de desempenho	Descrição
IOPS	Número médio de operações de entrada/saída que o SVM processa 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 às solicitações do aplicativo.
Volume	IOPS	Número médio de operações de entrada/saída que 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.	Taxa de perda de cache	Porcentagem média de solicitações de leitura de aplicativos cliente 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 do aplicativo.	Espaço de nomes	IOPS
Número médio de operações de entrada/saída processadas pelo namespace por segundo.	MB/s	Número médio de megabytes de dados transferidos de e para este namespace por segundo.
Latência	Número médio de milissegundos que o namespace leva para responder às solicitações do aplicativo.	Porta
Utilização de largura de banda	Porcentagem média da largura de banda disponível da porta que está sendo usada.	MB/s

Objeto de armazenamento	Contador de desempenho	Descrição
Número médio de megabytes de dados transferidos de e para esta porta por segundo.	Interface de rede (LIF)	MB/s

Quais objetos e contadores podem ser usados em políticas de limite de combinação

Somente alguns contadores de desempenho podem ser usados juntos em políticas combinadas. Quando 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 de armazenamento secundário e contador
Latência de volume	IOPS do volume
Volume MB/s	Utilização agregada
Capacidade de Desempenho Agregada Utilizada	Utilização de nós
Capacidade de desempenho do nó usada	Capacidade de desempenho do nó usada - aquisição
Latência de LUN	LUN IOPS
LUNMB/s	Utilização agregada
Capacidade de Desempenho Agregada Utilizada	Utilização de nós
Capacidade de desempenho do nó usada	Capacidade de desempenho do nó usada - aquisição



Quando uma política de combinação de volume é aplicada a um volume FlexGroup , em vez de a um FlexVol volume, somente os atributos “Volume IOPS” 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 FlexGroup podem existir em mais de um nó ou agregado.

Crie políticas de limite de desempenho definidas pelo usuário

Crie políticas de limite de desempenho para objetos de armazenamento para que 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

Você deve ter a função de Administrador do Aplicativo.

Crie 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 (chamado de *clonagem*).

Os valores limite válidos são de 0,001 a 10.000.000 para números, 0,001 a 100 para porcentagens e 0,001 a 200 para porcentagens de Capacidade de Desempenho Utilizada.



A versão atual fornece limites que enviam eventos quando um valor de contador excede a configuração de limite. Não é possível definir limites que enviem eventos quando um valor do contador cair abaixo de uma configuração de limite.

Passos

1. No painel de navegação esquerdo, selecione **Limites de evento > Desempenho**.

A página Limites de desempenho é exibida.

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...
Criar uma nova política	Criar
Clonar uma política existente	Selecione uma política existente e clique em Clonar

A página Criar política de limite de desempenho ou Clonar política de limite de desempenho é exibida.

3. Defina a política de limite especificando os valores de limite do contador de desempenho que você 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 Críticos.

Você deve definir pelo menos um Aviso ou um limite Crítico. Você não precisa definir os dois tipos de limites.

- c. Selecione um contador de desempenho secundário, se necessário, e especifique os valores limite para eventos de Aviso e Críticos.

Incluir 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 o período de tempo durante 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 retornará à página Limites de desempenho. Uma mensagem de sucesso no topo da página confirma que a política de limite foi criada e fornece um link para a página Inventário para esse tipo de objeto, para que você possa aplicar a nova política aos objetos de armazenamento imediatamente.

Se você quiser aplicar a nova política de limite aos objetos de armazenamento neste momento, clique no link **Ir para object_type agora** para ir para a página Inventário.

Atribuir políticas de limite de desempenho a objetos de armazenamento

Atribua uma política de limite de desempenho definida pelo usuário a um objeto de armazenamento para que o Unified Manager relate um evento se o valor do contador de desempenho exceder a configuração da política.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

A política ou políticas de limite de desempenho que você deseja aplicar ao objeto devem existir.

Você pode aplicar apenas uma política de desempenho por vez a um objeto ou a um grupo de objetos.

Você pode atribuir no máximo três políticas de limite a cada objeto de armazenamento. Ao atribuir políticas a vários objetos, se algum dos objetos já tiver o número máximo de políticas atribuídas, o Unified Manager executará as seguintes ações:

- Aplica a política a todos os objetos selecionados que não atingiram seu limite máximo
- Ignora os objetos que atingiram o número máximo de políticas
- Exibe uma mensagem informando que a política não foi atribuída a todos os objetos

Passos

1. Na página Inventário de desempenho de qualquer objeto de armazenamento, selecione o objeto ou objetos aos quais você deseja atribuir uma política de limite:

Para atribuir limites a...	Clique...
Um único objeto	A caixa de seleção à esquerda desse objeto.
Vários objetos	A caixa de seleção à esquerda de cada objeto.
Todos os objetos na página	O  caixa suspensa e escolha Selecionar todos os objetos nesta página.
Todos os objetos do mesmo tipo	O  caixa suspensa e escolha Selecionar todos os objetos.

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 **Atribuir política de limite de desempenho.**

A página Atribuir política de limite de desempenho é exibida, mostrando uma lista de políticas de limite

existentes para esse tipo específico de objeto de armazenamento.

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 **Atribuir política**.

Uma mensagem de sucesso no topo da página confirma que a política de limite foi atribuída ao objeto ou objetos e fornece um link para a página Alertas para que você possa configurar as definições de alerta para este objeto e política.

Se você quiser que alertas sejam enviados por e-mail ou como uma interceptação SNMP para notificá-lo de que um evento de desempenho específico foi gerado, você deve configurar as definições de alerta na página Configuração de alerta.

Ver políticas de limite de desempenho

Você pode visualizar todas as políticas de limite de desempenho definidas atualmente na página Limites de desempenho.

A lista de políticas de limite é classificada em ordem alfabética por nome da política e inclui políticas para todos os tipos de objetos de armazenamento. Você pode clicar em um cabeçalho de coluna para classificar as políticas por essa coluna. Se você estiver procurando por 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.

Etapa

1. No painel de navegação esquerdo, selecione **Limites de evento > Desempenho**.

A página Limites de desempenho é exibida.

Editar políticas de limite de desempenho definidas pelo usuário

Você pode editar as configurações de limite para políticas de limite de desempenho existentes. Isso pode ser útil se você perceber que está recebendo muitos ou poucos alertas para determinadas condições limite.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

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 **Limites de evento > Desempenho**.

A página Limites de desempenho é exibida.

2. Selecione a política de limite que você 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 retornará à página Limites de desempenho.

Depois de salvar, as alterações são atualizadas imediatamente em todos os objetos de armazenamento que usam a política.

Dependendo do tipo de alterações feitas na política, talvez você queira revisar as configurações de alerta definidas para os objetos que usam a política na página Configuração de alerta.

Remover políticas de limite de desempenho de objetos de armazenamento

Você pode remover uma política de limite de desempenho definida pelo usuário de um objeto de armazenamento quando não quiser mais que o Unified Manager monitore o valor do contador de desempenho.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Você pode remover apenas uma política por 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	Selecione a caixa de seleção à esquerda desse objeto.
Vários objetos	Selecione a caixa de seleção à esquerda de cada objeto.
Todos os objetos na página	Clique  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 da política será aplicada a todos os objetos de armazenamento que usam a política. 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 houver 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 do 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 se você visualizar 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 desempenho quando um objeto é movido

Como as políticas de limite de desempenho são atribuídas a objetos de armazenamento, se você mover um objeto, todas as políticas de limite atribuídas permanecerão anexadas ao objeto após a conclusão da movimentação. 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 nó — a condição de contador secundário será 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 alteração informativa. Um ícone de evento de alteração aparece na linha do tempo Eventos na página Performance Explorer e na página Análise de carga de trabalho para indicar o horário 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 após a conclusão da operação de movimentação. No entanto, 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 aquisição e devolução de HA

Quando uma operação de aquisição ou devolução ocorre em uma configuração de alta disponibilidade (HA),

os objetos que são movidos de um nó para outro 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 da alternância para o novo nó não é identificado até a próxima pesquisa da configuração do cluster.



Se uma operação de aquisição e devolução ocorrer dentro do período de coleta de alterações de configuração de 15 minutos, talvez você não veja as estatísticas de desempenho passarem 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 simples e combinadas são mantidas em todos os objetos, e a parte do nó da política de limite é aplicada ao novo nó.

Funcionalidade de política de limite durante a troca do MetroCluster

Objetos que são movidos de um cluster para outro em uma configuração MetroCluster não mantêm suas configurações de política de limite definidas pelo usuário. Se necessário, você pode aplicar políticas de limite nos volumes e LUNs que foram movidos para o cluster de parceiros. Depois que um objeto retorna ao seu cluster original, a política de limite definida pelo usuário é reaplicada automaticamente.

Para obter informações, consulte ["Comportamento do volume durante a comutação e o retorno"](#).

Analisar eventos de desempenho

Você pode analisar eventos de desempenho para identificar quando eles foram detectados, se estão ativos (novos ou reconhecidos) ou obsoletos, as cargas de trabalho e os componentes do cluster envolvidos e as opções para resolver os eventos por conta própria.

Exibir informações sobre eventos de desempenho

Você pode usar a página de inventário do Gerenciamento de Eventos para visualizar uma lista de todos os eventos de desempenho nos clusters monitorados pelo Unified Manager. Ao visualizar essas informações, você pode determinar os eventos mais críticos e, em seguida, obter informações detalhadas para determinar a causa do evento.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

A lista de eventos é classificada por hora detectada, com os eventos mais recentes listados primeiro. Você pode clicar no cabeçalho de uma coluna para classificar os eventos com base nessa coluna. Por exemplo, você pode classificar pela coluna Status para visualizar eventos por gravidade. Se você estiver procurando por um evento específico ou por 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 definida pelo usuário

- Política de limite de desempenho definida pelo sistema
- Limite de desempenho dinâmico

A coluna Tipo de evento lista a origem do evento. Você pode selecionar um evento para ver detalhes sobre ele na página Detalhes do evento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.
2. No menu Exibir, selecione **Eventos de desempenho ativos**.

A página exibe todos os eventos de desempenho novos e reconhecidos 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.

Analisar eventos a partir de limites de desempenho definidos pelo usuário

Eventos gerados a partir de limites definidos pelo usuário indicam que um contador de desempenho para um determinado objeto de armazenamento, 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.

Use a página Detalhes do evento para analisar o evento de desempenho e tomar medidas corretivas, se necessário, para retornar o desempenho ao normal.

Responder 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 ultrapassa um limite crítico ou de aviso definido pelo usuário. Você também pode usar o Unified Manager para verificar a integridade do componente do cluster e ver se eventos de integridade recentes detectados no componente contribuíram para o evento de desempenho.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Deve haver eventos de desempenho novos ou obsoletos.

Passos

1. Exiba a página **Detalhes do evento** para visualizar informações sobre o evento.
2. Revise a **Descrição**, que descreve a violação do limite que causou o evento.

Por exemplo, a mensagem “O valor de latência de 456 ms/op acionou um evento de AVISO com base 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 que está 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 **Horário de Acionamento do Evento** para que você possa investigar se outros eventos podem ter ocorrido ao mesmo tempo e que podem ter contribuído para este evento.
5. Siga uma das opções abaixo para investigar melhor o evento e determinar se você precisa executar alguma ação para resolver o problema de desempenho:

Opção	Possíveis ações de investigação
Clique no nome do objeto de origem para exibir a página do Explorer desse objeto.	Esta página permite que você visualize os detalhes do objeto e compare este objeto com outros objetos de armazenamento semelhantes para ver se outros objetos de armazenamento apresentam problemas de desempenho no mesmo período. Por exemplo, para ver se outros volumes no mesmo agregado também estão tendo problemas de desempenho.
Clique no nome do cluster para exibir a página Resumo do Cluster.	Esta página permite que você visualize os detalhes do cluster no qual este objeto reside para ver se outros problemas de desempenho ocorreram na mesma época.

Analisar eventos a partir de limites de desempenho definidos pelo sistema

Eventos gerados a partir de limites de desempenho definidos pelo sistema indicam que um contador de desempenho, ou conjunto de contadores de desempenho, para um determinado objeto de armazenamento ultrapassou o limite de uma política definida pelo sistema. Isso indica que o objeto de armazenamento, por exemplo, um agregado ou nó, está enfrentando um problema de desempenho.

Use a página 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 habilitadas nos sistemas Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select .

Responder a eventos de limite de desempenho definidos pelo sistema

Você pode usar o Unified Manager para investigar eventos de desempenho causados por um contador de desempenho que ultrapassa um limite de aviso definido pelo sistema. Você também pode usar o Unified Manager para verificar a integridade do componente do cluster e ver se eventos recentes detectados no componente contribuíram para o evento de desempenho.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Deve haver eventos de desempenho novos ou obsoletos.

Passos

1. Exiba a página **Detalhes do evento** para visualizar informações sobre o evento.
2. Revise a **Descrição**, que descreve a violação do limite que causou o evento.

Por exemplo, a mensagem “O valor de utilização do nó de 90% acionou um evento de AVISO com base na configuração de limite de 85%” indica que ocorreu um evento de aviso de utilização do nó para o objeto de cluster.

3. Anote o **Horário de Acionamento do Evento** para que você possa investigar se outros eventos podem ter ocorrido ao mesmo tempo e que podem ter contribuído para este evento.
4. Em **Diagnóstico do Sistema**, revise a breve descrição do tipo de análise que a política definida pelo sistema está executando no objeto do cluster.

Para alguns eventos, um ícone verde ou vermelho é exibido ao lado do diagnóstico para indicar se um problema foi encontrado naquele diagnóstico específico. Para outros tipos de eventos definidos pelo sistema, os gráficos de contagem exibem o desempenho do objeto.

5. Em **Ações sugeridas**, clique no link **Ajude-me a fazer isso** para ver as ações sugeridas que você pode executar para tentar resolver o evento de desempenho por conta própria.

Responder 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 carga de trabalho (IOPS, IOPS/TB ou MBps) excede a configuração de política de QoS do ONTAP definida e a latência da carga de trabalho está sendo afetada. Esses eventos definidos pelo sistema oferecem a oportunidade de corrigir possíveis problemas de desempenho antes que muitas cargas de trabalho sejam afetadas pela latência.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Deve haver eventos de performance novos, reconhecidos ou obsoletos.

O Unified Manager gera eventos de aviso para violações de política de QoS quando a taxa de transferência de carga de trabalho excede a configuração de política de QoS definida durante cada período de coleta de desempenho da hora anterior. A taxa de transferência da carga de trabalho pode exceder o limite de QoS por apenas um curto período de tempo durante cada período de coleta, mas o Unified Manager exibe apenas a taxa de transferência "média" durante o período de coleta no gráfico. Por esse motivo, você pode receber eventos de QoS mesmo que a taxa de transferência de uma carga de trabalho não tenha ultrapassado o limite da 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
- Adicionar ou remover cargas de trabalho em um grupo de políticas

- Movendo uma carga de trabalho entre grupos de políticas
- Alterando o limite de taxa de transferência de um grupo de políticas
- Mover uma carga de trabalho para um agregado ou nó diferente

Passos

1. Exiba a página **Detalhes do evento** para visualizar informações sobre o evento.
2. Revise a **Descrição**, que descreve a violação do limite que causou o evento.

Por exemplo, a mensagem “O valor de IOPS de 1.352 IOPS no vol1_NFS1 acionou um evento de AVISO para identificar possíveis problemas de desempenho para a carga de trabalho” indica que um evento de QoS Max IOPS ocorreu no volume vol1_NFS1.

3. Revise a seção **Informações do evento** para ver mais detalhes sobre quando o evento ocorreu e há quanto tempo ele está ativo.

Além disso, para volumes ou LUNs que compartilham a taxa de transferência de uma política de QoS, você pode ver os nomes das três principais cargas de trabalho que estão consumindo mais IOPS ou MBps.

4. Na seção **Diagnóstico do Sistema**, revise os dois gráficos: um para IOPS ou MBps médios totais (dependendo do evento) e um para latência. Quando organizado dessa forma, você pode ver quais componentes do cluster estão afetando mais a latência quando a carga de trabalho se aproxima do limite máximo de QoS.

Para um evento de política de QoS compartilhada, as três principais cargas de trabalho são mostradas no gráfico de taxa de transferência. Se mais de três cargas de trabalho estiverem compartilhando a política de QoS, cargas de trabalho adicionais serão adicionadas em uma categoria “Outras cargas de trabalho”. Além disso, o gráfico de latência mostra a latência média em todas as cargas de trabalho que fazem parte da política de QoS.

Observe que, para eventos de política de QoS adaptável, os gráficos de IOPS e MBps mostram valores de IOPS ou MBps que o ONTAP converteu da política 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.

Entenda eventos de políticas de QoS adaptáveis que têm um tamanho de bloco definido

Os grupos de políticas de QoS adaptáveis dimensionam automaticamente um teto ou piso de taxa de transferência 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.

Atribuir um limite de IOPS em uma política de QoS adaptável impõe um limite apenas ao número de operações que ocorrem em cada carga de trabalho. 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 nos 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 tiver uma média de 3.000 IOPS e o tamanho do bloco no cliente estiver definido como 32 KB, o MB/s efetivo para essa carga de trabalho será 96. Se essa mesma carga de trabalho tiver uma média de 3.000 IOPS e o tamanho do bloco no cliente estiver definido como 48 KB, então o MB/s efetivo para essa carga de trabalho será 144. Você pode ver que o nó está processando 50% mais dados quando o tamanho do bloco é maior.

Vejamos a seguinte política de QoS adaptável que tem um tamanho de bloco definido e como os eventos são acionados com base no tamanho de bloco definido no cliente.

Crie uma política e defina o pico de transferência para 2.500 IOPS/TB com um tamanho de bloco de 32 KB. Isso efetivamente define o limite de MB/s para 80 MB/s $((2500 \text{ IOPS} * 32 \text{ KB}) / 1000)$ para um volume com capacidade utilizada de 1 TB. Observe que o Unified Manager gera um evento de aviso quando o valor da taxa de transferência é 10% menor que o limite definido. Os eventos são gerados nas seguintes situações:

Capacidade Utilizada	O evento é gerado quando a taxa de transferência excede esse 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 2 TB do espaço disponível, o IOPS for 4.000 e o tamanho do bloco de QoS estiver definido como 32 KB no cliente, a taxa de transferência de MB/s será de 128 MB/s $((4.000 \text{ IOPS} * 32 \text{ KB}) / 1.000)$. Nenhum evento é gerado neste cenário porque 4.000 IOPS e 128 MB/s estão abaixo do limite para um volume que está usando 2 TB de espaço.

Se o volume estiver usando 2 TB do espaço disponível, o IOPS for 4.000 e o tamanho do bloco de QoS estiver definido como 64 KB no cliente, a taxa de transferência de MB/s será de 256 MB/s $((4.000 \text{ IOPS} * 64 \text{ KB}) / 1.000)$. Neste caso, os 4.000 IOPS não geram um evento, mas o valor de 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 inclui 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 tanto para IOPS quanto para MB/s, você receberá dois eventos.

Para obter mais informações sobre como ajustar as configurações de QoS, consulte ["Visão geral da gestão de desempenho"](#).

Responder a eventos de desempenho de superutilização de recursos do nó

O Unified Manager gera eventos de aviso de superutilização de recursos de nó quando

um único nó está operando acima dos limites de sua eficiência operacional e, portanto, potencialmente afetando as latências da carga de trabalho. Esses eventos definidos pelo sistema oferecem a oportunidade de corrigir possíveis problemas de desempenho antes que muitas cargas de trabalho sejam afetadas pela latência.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Deve haver eventos de desempenho novos ou obsoletos.

O Unified Manager gera eventos de aviso para violações de políticas de superutilização de recursos de nós, procurando por nós que estão usando mais de 100% de sua capacidade de desempenho por mais de 30 minutos.

Você pode usar o Gerenciador do Sistema ou os comandos ONTAP para corrigir esse tipo de problema de desempenho, incluindo as seguintes tarefas:

- Criar e aplicar uma política de QoS a quaisquer volumes ou LUNs que estejam usando excessivamente os recursos do sistema
- Reduzir o limite máximo de taxa de transferência de QoS de um grupo de políticas ao qual cargas de trabalho foram aplicadas
- Mover uma carga de trabalho 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 visualizar informações sobre o evento.
2. Revise a **Descrição**, que descreve a violação do limite que causou o evento.

Por exemplo, a mensagem “Perf. O valor de capacidade usada de 139% no simplicity-02 acionou um evento de AVISO para identificar possíveis problemas de desempenho na unidade de processamento de dados.” indica que a capacidade de desempenho no nó simplicity-02 está sendo usada em excesso e afetando o desempenho do nó.

3. Na seção **Diagnóstico do Sistema**, revise os três gráficos: um para capacidade de desempenho usada no nó, um para IOPS de armazenamento médio usado pelas principais cargas de trabalho e um para latência nas principais cargas de trabalho. Quando organizados dessa forma, você pode ver quais cargas de trabalho são a causa da latência no nó.

Você pode visualizar quais cargas de trabalho têm políticas de QoS aplicadas e quais não, movendo o cursor sobre o gráfico de 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.

Responder a eventos de desempenho de desequilíbrio de 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 da carga de trabalho. Esses eventos definidos pelo sistema oferecem a oportunidade de corrigir possíveis problemas de desempenho antes que muitas cargas de trabalho sejam afetadas pela latência.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

O Unified Manager gera eventos de aviso para violações de política de limite de desequilíbrio de cluster comparando o valor de capacidade de desempenho usada para todos os nós no cluster para ver se há uma diferença de carga de 30% entre quaisquer nós.

Estas etapas ajudam a identificar os seguintes recursos para que você possa mover cargas de trabalho de alto desempenho para um nó com menor utilização:

- 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 visualizar informações sobre o evento.
2. Revise a **Descrição**, que descreve a violação do limite que causou o evento.

Por exemplo, a mensagem “O contador de capacidade de desempenho usada indica uma diferença de carga de 62% entre os nós no cluster Dallas-1-8 e disparou um evento de AVISO com base no limite do sistema de 30%” indica que a capacidade de desempenho em um dos nós está sendo usada em excesso 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 alta capacidade de desempenho usada para um nó com o menor valor de capacidade de desempenho usada.
4. Identifique os nós com maior e menor valor de capacidade de desempenho utilizada:
 - a. Na seção **Informações do evento**, clique no nome do cluster de origem.
 - b. Na página **Cluster / Resumo de desempenho**, clique em **Nós** na área **Objetos gerenciados**.
 - c. Na página de inventário **Nós**, classifique os nós pela coluna **Capacidade de desempenho usada**.
 - d. Identifique os nós com maior e menor valor de capacidade de desempenho utilizado e anote esses nomes.
5. Identifique o volume que usa mais IOPS no nó que tem o maior valor de capacidade de desempenho usada:
 - a. Clique no nó com o maior valor de capacidade de desempenho utilizado.
 - b. Na página **Node / Performance Explorer**, selecione **Agregados neste nó** no menu **Exibir e comparar**.
 - c. Clique no agregado com o maior valor de capacidade de desempenho utilizada.
 - d. Na página **Aggregate / Performance Explorer**, selecione **Volumes neste agregado** no menu **View and Compare**.
 - e. Classifique os volumes pela coluna **IOPS** e anote o nome do volume que usa o maior número de 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 utilizada:

- a. Clique em **Armazenamento > Agregados** para exibir a página de inventário **Agregados**.
 - b. Selecione a visualização **Desempenho: Todos os agregados**.
 - c. Clique no botão **Filtro** e adicione um filtro onde “Nó” seja igual ao nome do nó com o menor valor de capacidade de desempenho usado que você anotou na etapa 4.
 - d. Escreva o nome do agregado que apresenta o menor valor de capacidade de desempenho utilizada.
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 de movimentação usando o ONTAP System Manager, o OnCommand Workflow Automation, os comandos ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, verifique se você está recebendo o mesmo evento de desequilíbrio de cluster deste cluster.

Analisar eventos a partir de limites de desempenho dinâmico

Eventos gerados a partir de limites dinâmicos indicam que o tempo de resposta real (latência) para uma carga de trabalho é muito alto ou muito baixo em comparação ao intervalo de tempo de resposta esperado. Use a página Detalhes do evento para analisar o evento de desempenho e tomar medidas corretivas, se necessário, para retornar o desempenho ao normal.



Limites de desempenho dinâmico não estão habilitados nos sistemas Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select .

Identificar cargas de trabalho de vítimas envolvidas em um evento de desempenho dinâmico

No Unified Manager, você pode identificar quais cargas de trabalho de volume têm o maior desvio no tempo de resposta (latência) causado por um componente de armazenamento em contenção. Identificar essas cargas de trabalho ajuda você a entender por que os aplicativos clientes que as acessam estão com desempenho mais lento que o normal.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Deve haver eventos de desempenho dinâmico novos, reconhecidos ou obsoletos.

A página Detalhes do evento exibe uma lista das cargas de trabalho definidas pelo usuário e pelo sistema, classificadas pelo maior desvio na atividade ou uso no componente ou mais impactadas pelo evento. Os valores são baseados nos picos que o Unified Manager identificou quando detectou e analisou o evento pela última vez.

Passos

1. Exiba a página **Detalhes do evento** para visualizar informações sobre o evento.
2. Nos gráficos Latência da carga de trabalho e Atividade da carga de trabalho, selecione **Cargas de trabalho da vítima**.
3. Passe o cursor sobre os gráficos para visualizar as principais cargas de trabalho definidas pelo usuário

que estão afetando o componente e o nome da carga de trabalho da vítima.

Identificar cargas de trabalho agressivas envolvidas em um evento de desempenho dinâmico

No Unified Manager, você pode identificar quais cargas de trabalho têm o maior desvio no uso de um componente de cluster em contenção. Identificar essas cargas de trabalho ajuda você a entender por que certos volumes no cluster têm tempos de resposta lentos (latência).

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Deve haver eventos de desempenho dinâmico novos, reconhecidos ou obsoletos.

A página Detalhes do evento exibe uma lista das cargas de trabalho definidas pelo usuário e pelo sistema, classificadas pelo maior uso do componente ou mais impactadas pelo evento. Os valores são baseados nos picos que o Unified Manager identificou quando detectou e analisou o evento pela última vez.

Passos

1. Exiba a página Detalhes do evento para visualizar informações sobre o evento.
2. Nos gráficos Latência da carga de trabalho e Atividade da carga de trabalho, selecione **Cargas de trabalho agressivas**.
3. Passe o cursor sobre os gráficos para visualizar as principais cargas de trabalho de intimidação definidas pelo usuário que estão afetando o componente.

Identificar cargas de trabalho de tubarão envolvidas em um evento de desempenho dinâmico

No Unified Manager, você pode identificar quais cargas de trabalho têm o maior desvio no uso de um componente de armazenamento em contenção. Identificar essas cargas de trabalho ajuda a determinar se elas devem ser movidas para um cluster menos utilizado.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Existem eventos dinâmicos de desempenho novos, reconhecidos ou obsoletos.

A página Detalhes do evento exibe uma lista das cargas de trabalho definidas pelo usuário e pelo sistema, classificadas pelo maior uso do componente ou mais impactadas pelo evento. Os valores são baseados nos picos que o Unified Manager identificou quando detectou e analisou o evento pela última vez.

Passos

1. Exiba a página **Detalhes do evento** para visualizar informações sobre o evento.
2. Nos gráficos Latência da carga de trabalho e Atividade da carga de trabalho, selecione **Cargas de trabalho do Shark**.
3. Passe o cursor sobre os gráficos para visualizar as principais cargas de trabalho definidas pelo usuário que estão afetando o componente e o nome da carga de trabalho do tubarão.

Análise de eventos de desempenho 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 revisar as ações sugeridas para resolvê-lo.

Os eventos de desempenho do MetroCluster podem ser devido a cargas de trabalho *bully* que estão utilizando excessivamente os links de interconexão (ISLs) entre os clusters ou devido a problemas de integridade do link. O Unified Manager monitora cada cluster em uma configuração do MetroCluster de forma independente, sem considerar eventos de desempenho em um cluster parceiro.

Os eventos de desempenho de ambos os clusters na configuração do MetroCluster também são exibidos na página do Painel do Unified Manager. Você também pode visualizar as páginas de integridade do Unified Manager para verificar a integridade de cada cluster e visualizar seu relacionamento.

Analisar um evento de desempenho dinâmico em um cluster em uma configuração MetroCluster

Você pode usar o Unified Manager para analisar o cluster em uma configuração do MetroCluster na qual um evento de desempenho foi detectado. Você pode identificar o nome do cluster, o tempo de detecção do evento e as cargas de trabalho *bully* e *victim* envolvidas.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos 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 devem ser monitorados pela mesma instância do Unified Manager.

Passos

1. Exiba a página **Detalhes do evento** para visualizar 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 está vermelho, indicando que os recursos do MetroCluster estão em contenção. Posicione o cursor sobre o ícone para exibir uma descrição do ícone.

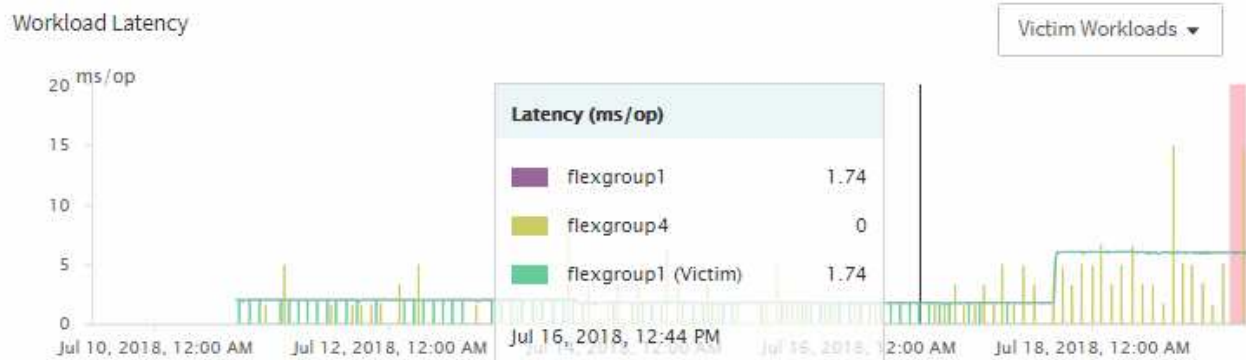


3. Anote o nome do cluster e o horário de detecção do evento, que você pode usar para analisar eventos de desempenho no cluster parceiro.
4. Nos gráficos, revise as cargas de trabalho das *vítimas* para confirmar se seus tempos de resposta são maiores que o limite de desempenho.

Neste exemplo, a carga de trabalho da vítima é exibida no texto flutuante. Os gráficos de latência exibem, em alto nível, um padrão de latência consistente para as cargas de trabalho das vítimas envolvidas. Embora a latência anormal das cargas de trabalho das vítimas tenha acionado o evento, um padrão de latência consistente pode indicar que as cargas de trabalho estão funcionando dentro do intervalo

esperado, mas que um pico de E/S aumentou a latência e acionou o evento.

^ System Diagnosis (Jul 9, 2018, 11:09 AM - Jul 19, 2018, 7:39 AM) ?



Se você instalou recentemente um aplicativo em um cliente que acessa essas cargas de trabalho de volume e esse aplicativo envia uma grande quantidade de E/S para eles, você pode estar prevendo que suas latências aumentarão. Se a latência das cargas de trabalho retornar ao intervalo esperado, o estado do evento mudar para obsoleto e permanecer nesse estado por mais de 30 minutos, você provavelmente poderá ignorar o evento. Se o evento estiver em andamento e permanecer no novo estado, você poderá investigá-lo mais detalhadamente para determinar se outros problemas causaram o evento.

5. No gráfico Taxa de transferência de carga de trabalho, selecione **Cargas de trabalho agressivas** para exibir as cargas de trabalho agressivas.

A presença de cargas de trabalho agressivas indica que o evento pode ter sido causado por uma ou mais cargas de trabalho no cluster local que estão utilizando excessivamente os recursos do MetroCluster. As cargas de trabalho de intimidação têm um alto desvio na taxa de transferência de gravação (MB/s).

Este 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 gravação MB/s para identificar uma taxa de transferência anormal, o que pode indicar que uma carga de trabalho está utilizando excessivamente os recursos do MetroCluster.

Se nenhuma carga de trabalho de intimidação estiver envolvida 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 parceiro. Você pode usar o Unified Manager para verificar a integridade de ambos os clusters em uma configuração do MetroCluster. Você também pode usar o Unified Manager para verificar e analisar eventos de desempenho no cluster de parceiros.

Analisar um evento de desempenho dinâmico para um cluster remoto em uma configuração MetroCluster

Você pode usar o Unified Manager para analisar eventos de desempenho dinâmico 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 parceiro.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter analisado um evento de desempenho em um cluster local em uma configuração MetroCluster e obtido o tempo de detecção do evento.
- Você deve ter verificado a integridade do cluster local e do cluster parceiro envolvido no evento de desempenho e obtido o nome do cluster parceiro.

Passos

1. Efetue 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 **Última hora** e clique em **Aplicar intervalo**.
4. No seletor **Filtragem**, selecione **Cluster** no menu suspenso à esquerda, digite o nome do cluster parceiro no campo de texto e clique em **Aplicar filtro**.

Se não houver eventos para o cluster selecionado na última hora, isso indica que o cluster não apresentou problemas de desempenho durante o tempo em que o evento foi detectado em seu parceiro.

5. Se o cluster selecionado tiver eventos detectados na última hora, compare o tempo de detecção do evento com o tempo de detecção do evento no cluster local.

Se esses eventos envolverem cargas de trabalho agressivas causando contenção no componente de processamento de dados, um ou mais desses agressores 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 **Detalhes do evento**.

Se esses eventos não envolverem cargas de trabalho agressivas, eles não causaram o evento de desempenho no cluster local.

Responder 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 desempenho causado por um grupo de políticas de Qualidade de Serviço (QoS) que limita a taxa de transferência de carga de trabalho (MB/s). A limitação 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

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Deve haver eventos de performance novos, reconhecidos ou obsoletos.

Passos

1. Exiba a página **Detalhes do evento** para visualizar informações sobre o evento.
2. Leia a **Descrição**, que exibe o nome das cargas de trabalho impactadas pela limitação.



A descrição pode exibir a mesma carga de trabalho para a vítima e o agressor, porque a limitação faz com que a carga de trabalho seja vítima de si mesma.

3. Registre o nome do volume usando um aplicativo como um editor de texto.

Você pode pesquisar pelo nome do volume para localizá-lo mais tarde.

4. Nos gráficos **Latência da carga de trabalho** e **Utilização da carga de trabalho**, selecione **Cargas de trabalho agressivas**.
5. Passe o cursor sobre os gráficos para visualizar as principais cargas de trabalho definidas pelo usuário

que estão afetando o grupo de políticas.

A carga de trabalho no topo da lista tem o maior desvio e causou a ocorrência da limitação. A atividade é a porcentagem do limite do grupo de políticas usada por cada carga de trabalho.

6. Na área **Ações sugeridas**, clique no botão **Analisar carga de trabalho** para a carga de trabalho principal.
7. Na página Análise de carga de trabalho, defina o gráfico Latência para visualizar todos os componentes do cluster e o gráfico Taxa de transferência para visualizar o detalhamento.

Os gráficos de detalhamento são exibidos no gráfico de Latência e no gráfico de IOPS.

8. Compare os Limites de QoS no gráfico **Latência** para ver qual 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 contidas 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 de leitura/gravação** com os valores de **Leitura/gravação/outros**.

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 taxa de transferência ou um número alto 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 ONTAP System Manager 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 Repartição de rendimento.

O gráfico Leituras/gravações/outros é exibido.

13. No topo da página, aponte o cursor para o ícone de evento de alteração () para a alteração do limite do grupo de políticas.
14. Compare o gráfico **Leituras/gravações/outros** com o gráfico **Latência**.

As solicitações de leitura e gravação são as mesmas, mas a limitação foi interrompida e a latência diminuiu.

Responder a um evento de desempenho dinâmico causado por uma falha de disco

Você pode usar o Unified Manager para investigar um evento de desempenho causado por cargas de trabalho que utilizam excessivamente um agregado. Você também pode usar o Unified Manager para verificar a integridade do agregado e ver se eventos de integridade recentes detectados no agregado contribuíram para o evento de desempenho.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Deve haver eventos de performance novos, reconhecidos ou obsoletos.

Passos

1. Exiba a página **Detalhes do evento** para visualizar 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 impactada pelo componente do cluster em contenção. O agregado, que está no meio de uma reconstrução RAID para substituir o disco com falha por um disco reserva, é o componente do cluster em disputa. Em Componente em Contenção, o ícone Agregado é destacado em vermelho e o nome do agregado é exibido entre parênteses.

3. No gráfico Utilização da carga de trabalho, selecione **Cargas de trabalho intensas**.
4. Passe o cursor sobre o gráfico para visualizar as principais cargas de trabalho agressivas que estão afetando o componente.

As principais cargas de trabalho com maior pico de utilização desde que o evento foi detectado são exibidas na parte superior do gráfico. Uma das principais cargas de trabalho é a carga de trabalho definida pelo sistema Disk Health, que indica uma reconstrução RAID. Uma reconstrução é o processo interno envolvido na reconstrução do agregado com o disco sobressalente. A carga de trabalho do Disk Health, juntamente com outras cargas de trabalho no agregado, provavelmente causou a contenção no agregado e o evento associado.

5. Após confirmar que a atividade da carga de trabalho do Disk Health causou o evento, aguarde aproximadamente 30 minutos para que a reconstrução seja concluída e para que o Unified Manager analise o evento e detecte se o agregado ainda está em contenção.
6. Atualize os **Detalhes do evento**.

Após a conclusão da reconstrução do RAID, verifique se o Estado está obsoleto, indicando que o evento foi resolvido.

7. No gráfico Utilização da carga de trabalho, selecione **Cargas de trabalho intensas** para visualizar as cargas de trabalho agregadas por pico de utilização.
8. Na área **Ações sugeridas**, clique no botão **Analisar carga de trabalho** para a carga de trabalho principal.
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 do Evento, um ponto vermelho (●) indica quando ocorreu o evento de falha do disco.

10. No gráfico Utilização de Nós e Agregados, oculte a linha das estatísticas de Nós para que apenas a linha Agregados 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 alta quantidade de atividade de leitura e gravação, causada pelos processos de reconstrução do RAID, o que aumentou a latência do volume selecionado. Algumas horas após o evento, tanto as leituras quanto as gravações e a latência diminuíram, confirmando que o agregado não está mais em disputa.

Responder a um evento de desempenho dinâmico causado pela aquisição do HA

Você pode usar o Unified Manager para investigar um evento de desempenho causado pelo alto processamento de dados em um nó de cluster que está em um par de alta disponibilidade (HA). Você também pode usar o Unified Manager para verificar a integridade dos nós e ver se algum evento de integridade recente detectado nos nós contribuiu para o evento de desempenho.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Deve haver eventos de performance novos, reconhecidos ou obsoletos.

Passos

1. Exiba a página **Detalhes do evento** para visualizar 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 vítima cuja latência foi impactada pelo componente do cluster em contenção. O nó de processamento de dados, que assumiu todas as cargas de trabalho de seu nó parceiro, é o componente do cluster em disputa. Em Componente em Contenção, o ícone Data Processing é destacado em vermelho e o nome do nó que estava manipulando o processamento de dados no momento do evento é exibido entre parênteses.

3. Na **Descrição**, clique no nome do volume.

A página Volume Performance Explorer é exibida. No topo da página, na linha do tempo de Eventos, um ícone de evento de alteração () indica o horário em que o Unified Manager detectou o início da aquisição do HA.

4. Aponte o cursor para o ícone do evento de alteração para a aquisição do HA e os detalhes sobre a aquisição do HA serão exibidos no texto flutuante.

No gráfico de latência, um evento indica que o volume selecionado ultrapassou o limite de desempenho devido à alta latência, quase no mesmo momento da aquisição do HA.

5. Clique em **Visualização de Zoom** para exibir o gráfico de Latência em uma nova página.
6. No menu Exibir, selecione **Componentes do cluster** para visualizar a latência total por componente do cluster.
7. Aponte o cursor do mouse para o ícone do evento de alteração para o início da aquisição do HA e compare a latência do processamento de dados com a latência total.

No momento da aquisição da HA, houve um pico no processamento de dados devido ao aumento da demanda de carga de trabalho no nó de processamento de dados. O aumento da utilização da CPU aumentou a latência e disparou o evento.

8. Depois de corrigir o nó com falha, use o ONTAP System Manager para executar um retorno de HA, que move as cargas de trabalho do nó parceiro para o nó corrigido.
9. Após a conclusão da devolução do HA, após a próxima descoberta de configuração no Unified Manager (aproximadamente 15 minutos), localize o evento e a carga de trabalho acionados pela aquisição do HA na página de inventário **Gerenciamento de Eventos**.

O evento acionado pela aquisição do HA agora tem um estado obsoleto, o que indica que o evento foi resolvido. A latência no componente de processamento de dados diminuiu, o que diminuiu a latência total. O nó que o volume selecionado está usando para processamento de dados resolveu o evento.

Resolver eventos de desempenho

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 **Ajude-me a fazer isso** fornecem informações adicionais para cada ação sugerida, incluindo instruções para executar uma ação específica. Algumas das ações podem envolver o uso do Unified Manager, do ONTAP System Manager, do OnCommand Workflow Automation, dos comandos ONTAP CLI ou de uma combinação dessas ferramentas.

Confirme se a latência está dentro do intervalo esperado

Quando um componente de cluster está em contenção, as cargas de trabalho de volume que o utilizam podem ter tempo de resposta reduzido (latência). Você pode revisar a latência de cada carga de trabalho da vítima no componente em contenção para confirmar se sua latência real está dentro do intervalo esperado. Você também pode clicar no nome de um volume para visualizar 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 ao intervalo esperado.

Analise o impacto das alterações de configuração no desempenho da carga de trabalho

Alterações de configuração no cluster, como falha de disco, failover de HA ou movimentação de volume, podem afetar negativamente o desempenho do volume e causar aumento de latência.

No Unified Manager, você pode revisar a página Análise de carga de trabalho 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 da carga de trabalho do volume selecionado.

As páginas de desempenho do Unified Manager só podem detectar um número limitado de eventos de alteração. As páginas de saúde 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 no 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 alto número de solicitações de E/S para um volume específico no cluster, poderá melhorar o desempenho do cluster

ajustando o número de clientes que acessam 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 eles estão enviando mais E/S do que o normal, o que pode estar causando contenção em um componente do cluster. Na página Detalhes do evento, a seção Diagnóstico do sistema exibe as principais cargas de trabalho de volume usando o componente em contenção. Se você souber qual cliente está acessando um volume específico, poderá ir até 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 normal.

Em uma configuração do MetroCluster, as solicitações de gravação para um volume em um cluster local são espelhadas para 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 de ambos os clusters na configuração do MetroCluster. Ao reduzir as solicitações de gravação para esses volumes espelhados, os clusters podem executar menos operações de sincronização, o que reduz o impacto no desempenho em outras cargas de trabalho.

Verifique se há problemas de cliente ou de 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 em contenção, aumentar a latência das cargas de trabalho que o utilizam e acionar um evento no Unified Manager.

Na página Detalhes do evento, a seção Diagnóstico do sistema exibe as principais cargas de trabalho de volume usando o componente em contenção. Se você souber qual cliente está acessando um volume específico, poderá ir até 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 normal. Talvez seja necessário entrar em contato com o administrador do cliente ou com o fornecedor do aplicativo 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 terem um desempenho mais lento do que o esperado. Talvez seja necessário entrar em contato com o administrador da rede para obter assistência.

Verifique se outros volumes no grupo de política de QoS têm atividade excepcionalmente alta

Você pode revisar as cargas de trabalho no grupo de políticas de Qualidade de Serviço (QoS) com a maior alteração na atividade para determinar se mais de uma carga de trabalho causou o evento. Você também pode ver se outras cargas de trabalho ainda estão excedendo o limite de produtividade definido ou se elas estão de volta ao intervalo de atividade esperado.

Na página 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 maior alteração na atividade na parte superior da tabela. Essas cargas de trabalho podem ser os "valentões" cuja atividade excedeu o limite definido e podem ter causado o evento.

Você pode navegar até a página Análise de carga de trabalho para cada carga de trabalho de volume para revisar sua atividade de IOPS. Se a carga de trabalho tiver períodos de atividade operacional muito alta, isso 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 ONTAP System Manager ou os comandos ONTAP CLI para gerenciar grupos de políticas, da seguinte maneira:

- 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.
- Alterar 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 no ajuste de desempenho, além de reduzir o acesso indireto.

O acesso indireto pode reduzir a eficiência do sistema. Isso ocorre quando uma carga de trabalho de volume usa nós diferentes para processamento de rede e processamento de dados. Para reduzir o acesso indireto, você pode reorganizar os LIFs, o que envolve mover os LIFs para usar o mesmo nó para processamento de rede e processamento de dados. Você pode configurar o balanceamento de carga para que o ONTAP mova automaticamente LIFs ocupados para uma porta diferente ou pode mover um LIF manualmente.

Benefícios	Considerações
• Melhore o balanceamento de carga. • Reduza o acesso indireto.	 Ao mover um LIF conectado a compartilhamentos CIFS, os clientes que acessam os compartilhamentos CIFS são desconectados. Quaisquer solicitações de leitura ou gravação nos compartilhamentos CIFS são interrompidas.

Use os comandos ONTAP para configurar o balanceamento de carga. Para mais informações, consulte a documentação de rede ONTAP .

Use o ONTAP System Manager e os comandos ONTAP CLI para mover LIFs manualmente.

Execute operações de eficiência de armazenamento em horários de menor movimento

Você pode modificar a política ou a programação que lida com operações de eficiência de armazenamento para serem executadas quando as cargas de trabalho do volume afetado estiverem menos ocupadas.

As operações de eficiência de armazenamento podem usar uma grande quantidade de recursos de CPU do cluster e prejudicar os volumes nos quais as operações estão sendo executadas. Se os volumes das vítimas tiverem alta atividade ao mesmo tempo em que as operações de eficiência de armazenamento são executadas, sua latência pode aumentar e acionar um evento.

Na página 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 agressivas. Se você vir “eficiência de armazenamento” exibido próximo ao topo da tabela, essas operações estão intimidando as cargas de trabalho das vítimas. Ao modificar a política de eficiência ou o agendamento para execução quando essas cargas de trabalho estiverem menos ocupadas, você pode evitar que as operações de eficiência de armazenamento causem contenção em um cluster.

Você pode usar o ONTAP System Manager para gerenciar políticas de eficiência. Você pode usar os comandos ONTAP para gerenciar políticas e cronogramas de eficiência.

O que é eficiência de armazenamento

A eficiência de armazenamento permite que você armazene a quantidade máxima de dados pelo menor custo e acomoda o rápido crescimento de dados, consumindo menos espaço. A estratégia da NetApp para eficiência de armazenamento é baseada na fundação integrada de virtualização de armazenamento e armazenamento unificado fornecido pelo seu sistema operacional ONTAP principal e sistema de arquivos Write Anywhere File Layout (WAFL).

A eficiência de armazenamento inclui o uso de tecnologias como provisionamento fino, cópia de Snapshot, deduplicação, compactação de dados, FlexClone, replicação fina com SnapVault e volume SnapMirror, RAID-DP, Flash Cache, agregado Flash Pool e agregados habilitados para FabricPool, que ajudam a aumentar a utilização do armazenamento e diminuir os custos de armazenamento.

A arquitetura de armazenamento unificada permite que você consolide com eficiência uma rede de área de armazenamento (SAN), armazenamento conectado à rede (NAS) e armazenamento secundário em uma única plataforma.

Unidades de disco de alta densidade, como unidades Serial Advanced Technology Attachment (SATA) 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 HDD (começando com o ONTAP 9.8) como a camada de desempenho local e um armazenamento de objetos que você especifica como a camada de nuvem. Configurar o FabricPool ajuda você a gerenciar em qual camada de armazenamento (camada local ou camada de nuvem) os dados devem ser armazenados com base na frequência de acesso aos dados.

Tecnologias como provisionamento fino, cópia de Snapshot, deduplicação, compactação de dados, replicação fina com SnapVault e volume SnapMirror e FlexClone oferecem maiores economias. Você pode usar essas tecnologias individualmente ou em conjunto para atingir a máxima eficiência de armazenamento.

Adicionar discos e realocar dados

Você pode adicionar discos a um agregado para aumentar a capacidade de armazenamento e o desempenho desse agregado. Depois de adicionar os discos, você verá uma melhoria no desempenho de leitura somente após realocar os dados entre os discos adicionados.

Você pode usar estas instruções quando o Unified Manager receber eventos agregados acionados por limites dinâmicos ou por limites de desempenho definidos pelo sistema:

- Quando você recebe um evento de limite dinâmico, na página Detalhes do evento, o ícone do componente

do cluster que representa o agregado em contenção é destacado em vermelho.

Abaixo do ícone, entre parênteses, está o nome do agregado, que identifica o agregado ao qual você pode adicionar discos.

- Quando você recebe um evento de limite definido pelo sistema, na página Detalhes do evento, o texto da descrição do evento lista o nome do agregado que está apresentando o problema.

Você pode adicionar discos e realocar dados neste agregado.

Os discos que você adiciona 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 ONTAP System Manager ou os comandos ONTAP para adicionar discos a um agregado.



Você deve realocar dados somente ao usar agregados de HDD e Flash Pool. Não realoque dados em agregados SSD ou FabricPool.

Como habilitar o Flash Cache em um nó pode melhorar o desempenho da carga de trabalho

Você pode melhorar o desempenho da carga de trabalho habilitando o cache de dados inteligente do Flash Cache™ em cada nó do cluster.

Um módulo Flash Cache, ou módulo de memória baseado em PCIe do Performance Acceleration Module, 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 WAFL External Cache do ONTAP.

No Unified Manager, na página Detalhes do evento, o ícone do componente do cluster que representa o agregado em contenção é destacado em vermelho. Abaixo do ícone, entre parênteses, está o nome do agregado, que o identifica. Você pode habilitar o Flash Cache no nó em que o agregado reside.

Você pode usar o ONTAP System Manager ou os comandos ONTAP para verificar se o Flash Cache está instalado ou habilitado e habilitá-lo caso ainda não esteja. 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 Melhores Práticas de Cache Flash"](#)

Como habilitar o Flash Pool em um agregado de armazenamento pode melhorar o desempenho da carga de trabalho

Você pode melhorar o desempenho da carga de trabalho habilitando o recurso Flash Pool em um agregado. Um Flash Pool é um agregado que incorpora HDDs e SSDs. Os HDDs são usados para armazenamento primário e os SSDs fornecem um cache de leitura e gravação de alto desempenho para aumentar o desempenho agregado.

No Unified Manager, a página Detalhes do evento exibe o nome do agregado em contenção. Você pode usar o ONTAP System Manager ou os comandos ONTAP para verificar se o Flash Pool está habilitado para um agregado. Se você tiver SSDs instalados, poderá usar a interface de linha de comando para habilitá-los. Se

Se você tiver SSDs instalados, poderá executar o seguinte comando no agregado para verificar 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 em disputa.

Para obter mais informações sobre o Flash Pool e os requisitos para usá-lo, consulte o [Guia de gerenciamento de armazenamento físico do Clustered Data ONTAP](#).

Verificação de integridade da configuração do MetroCluster

Você pode usar o Unified Manager para revisar a integridade dos clusters em uma configuração do MetroCluster por IP ou FC. O status de integridade e os eventos ajudam a determinar se há problemas de hardware ou software que podem estar afetando o desempenho de suas cargas de trabalho.

Se você configurar o Unified Manager para enviar alertas por e-mail, poderá verificar seu e-mail em busca de quaisquer 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, em seguida, usar os filtros para exibir somente eventos de configuração do MetroCluster.

Para mais informações, consulte ["Verificando a integridade dos clusters em uma configuração MetroCluster"](#)

Verificação da configuração do MetroCluster

Você pode evitar problemas de desempenho para cargas de trabalho espelhadas em um MetroCluster por meio de configurações FC e IP, garantindo que a configuração do MetroCluster esteja definida corretamente. Você também pode melhorar o desempenho da carga de trabalho alterando a configuração ou atualizando componentes de software ou hardware.

Consulte ["Documentação do MetroCluster"](#) para obter instruções de configuração dos clusters na configuração do MetroCluster, incluindo os switches Fibre Channel (FC), cabos e links entre switches (ISLs). Ele também ajuda você a configurar o software MetroCluster para que os clusters locais e remotos possam se comunicar com dados de volume espelhados. Para obter informações específicas sobre a configuração do MetroCluster sobre IP, consulte ["Instalar uma configuração de IP do MetroCluster"](#).

Você pode comparar sua configuração do MetroCluster com os requisitos em ["Documentação do MetroCluster"](#) para determinar se a alteração ou atualização de componentes na configuração do MetroCluster pode melhorar o desempenho da carga de trabalho. Esta comparação pode ajudar você a responder às seguintes perguntas:

- Os controladores são apropriados para suas cargas de trabalho?
- Você precisa atualizar seus pacotes ISL para uma largura de banda maior para lidar com mais taxa de transferência?
- Você pode ajustar os créditos de buffer para buffer (BBC) em seus switches para aumentar a largura de banda?
- Se suas cargas de trabalho têm alta taxa de transferência de gravação no armazenamento de unidade de estado sólido (SSD), você precisa 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 o ["Documentação do MetroCluster"](#) .
- Para obter informações sobre a atualização de controladores, consulte ["Atualizando controladores em uma configuração MetroCluster FC usando switchover e switchback"](#) e ["Atualizando controladores em uma configuração de IP do MetroCluster usando switchover e switchback"](#)

Mover cargas de trabalho para um agregado diferente

Você pode usar o Unified Manager para ajudar a identificar um agregado que esteja menos ocupado do que o agregado onde suas cargas de trabalho residem atualmente e, então, você pode mover volumes ou LUNs selecionados para esse agregado. Mover cargas de trabalho de alto desempenho para um agregado menos ocupado, ou um agregado com armazenamento flash habilitado, permite que a carga de trabalho seja executada com mais eficiência.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter registrado o nome do agregado que está apresentando problemas de desempenho.
- Você deve ter registrado a data e a hora em que o agregado recebeu o evento.
- O Unified Manager deve ter coletado e analisado um mês ou mais de dados de desempenho.

Estas etapas ajudam a identificar os seguintes recursos para que você possa mover cargas de trabalho de alto desempenho para um agregado menos utilizado:

- 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 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 Desempenho/Aterrissagem do cluster.

- 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 pelos menos utilizados.

Você também pode identificar os agregados que têm a maior **Capacidade Livre**. Isso fornece uma lista de possíveis agregados para os quais você pode querer mover cargas de trabalho.

- 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 apresentando o problema de desempenho.

Os detalhes agregados são exibidos na página Performance/Aggregate Explorer.

- b. No seletor **Intervalo de tempo**, selecione **Últimos 30 dias** e 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 pelo maior MB/s e depois pelo maior IOPS para ver os volumes de 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 de movimentação usando o ONTAP System Manager, o OnCommand Workflow Automation, os comandos ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, verifique se você está recebendo o mesmo tipo de eventos deste nó ou agregado.

Mover cargas de trabalho 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 suas cargas de trabalho estão sendo executadas no momento e, então, você pode mover volumes selecionados para esse agregado. Mover cargas de trabalho de alto desempenho para um agregado em um nó menos ocupado permite que as cargas de trabalho em ambos os nós tenham um desempenho mais eficiente.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter registrado o nome do nó que está apresentando problemas de desempenho.
- Você deve ter registrado a data e a hora em que o nó recebeu o evento de desempenho.
- O Unified Manager deve ter coletado e analisado dados de desempenho por um mês ou mais.

Este procedimento ajuda você a identificar os seguintes recursos para que você possa mover cargas de trabalho de alto desempenho para um nó com menor utilização:

- Os nós no mesmo cluster que têm a maior capacidade de desempenho livre
- Os agregados no novo nó que têm a maior capacidade de desempenho 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 Desempenho/Aterrissagem do cluster.

- b. Na guia **Resumo**, clique em **Nós** no painel **Objetos gerenciados**.

A lista de nós neste cluster é exibida.

- c. 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.

- 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 esquerdo, clique em **Armazenamento > Agregados** e selecione **Desempenho > Todos os agregados** no menu Exibir.

A exibição Desempenho: Todos os agregados é exibida.

- b. Clique em **Filtragem**, selecione **Nó** no menu suspenso à esquerda, digite o nome do nó no campo de texto e clique em **Aplicar filtro**.

A exibição Desempenho: Todos os agregados é exibida novamente com a lista de agregados disponíveis neste nó.

- c. Clique na coluna **Capacidade de desempenho utilizada** para classificar os agregados pelos menos utilizados.

Isso fornece uma lista de possíveis agregados para os quais você pode querer mover cargas de trabalho.

- d. Anote o nome do agregado para o qual você deseja mover as cargas de trabalho.

3. Identifique as cargas de trabalho de alto desempenho do nó que recebeu o evento:

- a. Retorne para a 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 naquele 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 maior capacidade de desempenho livre no novo nó.

Você pode executar a operação de movimentação usando o ONTAP System Manager, o OnCommand Workflow Automation, os comandos ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, você pode verificar se está recebendo o mesmo tipo de eventos deste nó ou agregado.

Mover cargas de trabalho 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 onde suas cargas de trabalho estão

sendo executadas no momento e, então, você pode mover volumes selecionados para esse agregado. Mover cargas de trabalho de alto desempenho para um agregado em um nó menos ocupado permite que as cargas de trabalho em ambos os nós tenham um desempenho mais eficiente.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter registrado o nome do nó que está apresentando problemas de desempenho.
- Você deve ter registrado a data e a hora em que o nó recebeu o evento de desempenho.
- O Unified Manager deve ter coletado e analisado um mês ou mais de dados de desempenho.

Estas etapas ajudam a identificar os seguintes recursos para que você possa mover cargas de trabalho de alto desempenho para um nó com menor utilização:

- 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 Desempenho/Aterrissagem do cluster.

b. Na página **Resumo**, clique em **Nós** no painel **Objetos gerenciados**.

A lista de nós neste cluster é exibida.

c. Clique na coluna **Utilização** para classificar os nós pelos menos utilizados.

Você também pode identificar os nós que têm a maior **Capacidade Livre**. 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 esquerdo, clique em **Armazenamento > Agregados** e selecione **Desempenho > Todos os agregados** no menu Exibir.

A exibição Desempenho: Todos os agregados é exibida.

b. Clique em **Filtragem**, selecione **Nó** no menu suspenso à esquerda, digite o nome do nó no campo de texto e clique em **Aplicar filtro**.

A exibição Desempenho: Todos os agregados é exibida novamente com a lista de agregados disponíveis neste nó.

c. Clique na coluna **Utilização** para classificar os agregados pelos menos utilizados.

Você também pode identificar os agregados que têm a maior **Capacidade Livre**. Isso fornece uma lista de possíveis agregados para os quais você pode querer mover cargas de trabalho.

- d. Anote o nome do agregado para o qual você deseja mover as cargas de trabalho.
3. Identifique as cargas de trabalho de alto desempenho do nó que recebeu o evento:
 - a. Retorne para a página de detalhes do **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 naquele 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 baixa utilização no novo nó.

Você pode executar a operação de movimentação usando o ONTAP System Manager, o OnCommand Workflow Automation, os comandos ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, verifique se você está recebendo o mesmo tipo de eventos deste nó ou agregado.

Mover cargas de trabalho para um nó em um par de HA diferente

Você pode usar 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 desempenho livre do que o par de HA onde suas cargas de trabalho estão sendo executadas no momento. Em seguida, você pode mover volumes selecionados para agregados no novo par HA.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Seu cluster deve consistir em um mínimo de dois pares de HA

Você não pode usar esse processo de correção se tiver apenas um par de HA no seu cluster.

- Você deve ter registrado os nomes dos dois nós no par HA que estão apresentando problemas de desempenho.
- Você deve ter registrado a data e a hora em que os nós receberam o evento de desempenho.
- O Unified Manager deve ter coletado e analisado dados de desempenho por um mês ou mais.

Mover cargas de trabalho de alto desempenho para um agregado em um nó com mais capacidade de desempenho livre permite que as cargas de trabalho em ambos os nós tenham um desempenho mais eficiente. Este procedimento ajuda você a identificar os seguintes recursos para que você possa mover cargas de trabalho de alto desempenho para um nó que tenha mais capacidade de desempenho livre em um par de HA diferente:

- Os nós em um par de HA diferente no mesmo cluster que têm a maior capacidade de desempenho livre
- Os agregados nos novos nós que têm a maior capacidade de desempenho livre
- Os volumes de maior 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 Desempenho/Aterrissagem do cluster.
 - b. Na página **Resumo**, clique em **Nós** no painel **Objetos gerenciados**.

A lista de nós neste cluster é exibida na exibição Desempenho: Todos os nós.
 - c. Anote os nomes dos nós que estão em pares de HA diferentes do par de HA que está apresentando problemas de desempenho.
2. Identifique um nó no novo par HA que tenha a maior capacidade de desempenho livre:
 - 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 as cargas de trabalho.
3. Identifique um agregado no novo nó que tenha a maior capacidade de desempenho livre:
 - a. Na exibição **Desempenho: Todos os nós**, clique no nó.

Os detalhes do nó são exibidos na página Desempenho/Explorador de Nós.
 - 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 utilizada** para classificar os agregados pelos menos utilizados.

Isso fornece uma lista de possíveis agregados para os quais você pode querer mover cargas de trabalho.
 - d. Anote o nome do agregado para o qual você deseja mover as cargas de trabalho.
4. Identifique as cargas de trabalho de alto desempenho dos nós que receberam o evento:
 - a. Retorne para a página de detalhes do **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 naquele 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 deste evento para identificar possíveis volumes que você deseja mover desse nó também.
5. Mova os volumes para os agregados que você identificou como tendo maior capacidade de desempenho livre no novo nó.

Você pode executar a operação de movimentação usando o ONTAP System Manager, o OnCommand Workflow Automation, os comandos ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, você pode verificar se está recebendo o mesmo tipo de eventos deste nó ou agregado.

Mover cargas de trabalho para outro nó em um par de HA diferente

Você pode usar 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 onde suas cargas de trabalho estão sendo executadas no momento. Em seguida, você pode mover volumes selecionados para agregados no novo par HA. Mover cargas de trabalho de alto desempenho para um agregado em um nó menos ocupado permite que as cargas de trabalho em ambos os nós tenham um desempenho mais eficiente.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Seu cluster deve consistir em no mínimo dois pares de HA; você não pode usar esse processo de correção se tiver apenas um par de HA no seu cluster.
- Você deve ter registrado os nomes dos dois nós no par HA que estão apresentando problemas de desempenho.
- Você deve ter registrado a data e a hora em que os nós receberam o evento de desempenho.
- O Unified Manager deve ter coletado e analisado um mês ou mais de dados de desempenho.

Estas etapas ajudam a identificar os seguintes recursos para que você possa mover cargas de trabalho de alto desempenho para um nó com menor utilização em um par de HA diferente:

- Os nós em um par HA diferente no mesmo cluster que são menos utilizados
- Os agregados nos novos nós que são menos utilizados
- Os volumes de maior 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 **Armazenamento > Clusters** e selecione **Desempenho > Todos os Clusters** no menu Exibir.

A visualização Desempenho: Todos os clusters é exibida.
 - b. Clique no número no campo **Contagem de nós** do cluster atual.

A visualização Desempenho: Todos os nós é exibida.
 - c. Anote os nomes dos nós que estão em pares de HA diferentes do par de HA que está apresentando o problema de desempenho.
2. Identifique um nó no novo par HA que seja o menos utilizado:
 - a. Clique na coluna **Utilização** para classificar os nós pelos menos utilizados.

Você também pode identificar os nós que têm a maior **Capacidade Livre**. 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 esquerdo, clique em **Armazenamento > Agregados** e selecione **Desempenho > Todos os agregados** no menu Exibir.
- A exibição Desempenho: Todos os agregados é exibida.
- b. Clique em **Filtragem**, selecione **Nó** no menu suspenso à esquerda, digite o nome do nó no campo de texto e clique em **Aplicar filtro**.
- A exibição Desempenho: Todos os agregados é exibida novamente com a lista de agregados disponíveis neste nó.
- c. Clique na coluna **Utilização** para classificar os agregados pelos menos utilizados.
- Você também pode identificar os agregados que têm a maior **Capacidade Livre**. Isso fornece uma lista de possíveis agregados para os quais você pode querer mover cargas de trabalho.
- d. Anote o nome do agregado para o qual você deseja mover as cargas de trabalho.
4. Identifique as cargas de trabalho de alto desempenho dos nós que receberam o evento:
- a. Retorne para a página de detalhes do **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 naquele 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 deste evento para identificar possíveis volumes que você deseja mover desse nó também.
5. Mova os volumes para os agregados que você identificou como tendo baixa utilização no novo nó.
- Você pode executar a operação de movimentação usando o ONTAP System Manager, o OnCommand Workflow Automation, os comandos ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, verifique se você está recebendo o mesmo tipo de eventos deste nó ou agregado.

Use as configurações de política de QoS para priorizar o trabalho neste 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 as cargas de trabalho que ele contém. Se as cargas de trabalho estiverem em um grupo de políticas sem limite definido, como o grupo de políticas padrão, ou se 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 excessivamente os

recursos do nó, a descrição do evento na página 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 cargas de trabalho têm o maior uso, o que pode ter contribuído para o evento.

Ao atribuir os volumes que estão usando excessivamente os recursos do nó a uma configuração de grupo de políticas mais restritiva, o grupo de políticas limita as cargas de trabalho para restringir sua atividade, o que pode reduzir o uso dos recursos naquele nó.

Você pode usar o ONTAP System Manager ou os comandos ONTAP para gerenciar grupos de políticas, incluindo as seguintes tarefas:

- Criando um grupo de políticas
- Adicionar ou remover cargas de trabalho em um grupo de políticas
- Movendo uma carga de trabalho entre grupos de políticas
- Alterando o limite de taxa de transferência de um grupo de políticas

Remover volumes e LUNs inativos

Quando o espaço livre agregado for identificado como um problema, você poderá procurar 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 desempenho 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 visualização Desempenho: Todos os volumes. A partir daí, você pode classificar os volumes afetados por **IOPS** para ver quais volumes não estavam ativos.

Para identificar LUNs não utilizados:

1. Na página 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 **Filtragem**, selecione **Agregado** no menu suspenso à esquerda, digite o nome do agregado no campo de texto e clique em **Aplicar filtro**.
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 ONTAP System Manager ou os comandos ONTAP para excluir esses objetos.

Adicionar discos e executar reconstrução de layout agregado

Você pode adicionar discos a um agregado para aumentar a capacidade de armazenamento e o desempenho desse agregado. Após adicionar os discos, você só verá uma melhoria no desempenho após reconstruir o agregado.

Quando você recebe um evento de limite definido pelo sistema na página Detalhes do evento, o texto da descrição do evento lista o nome do agregado que está apresentando o problema. Você pode adicionar discos e reconstruir dados neste agregado.

Os discos que você adiciona 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 ONTAP System Manager ou os comandos ONTAP para adicionar discos a um agregado.

["Relatório Técnico 3838: Guia de Configuração do Subsistema de Armazenamento"](#)

Configurar 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 do cluster para um servidor externo para que os gerentes de armazenamento possam mapear 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 denominada "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 desempenho de todos os clusters que 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	Estatísticas de desempenho de alto nível para os seguintes objetos: • LUNs • Volumes	Este grupo fornece IOPS ou latência total para todos os LUNs e volumes em todos os clusters monitorados. Este grupo fornece o menor número de estatísticas.
Utilização de Recursos	Estatísticas de utilização de recursos para os seguintes objetos: • Nós • Agregados	Este grupo fornece estatísticas de utilização para o nó e recursos físicos agregados em todos os clusters monitorados. Ele também fornece as estatísticas coletadas no grupo Monitor de Desempenho.

Grupo de estatísticas	Dados incluídos	Detalhes
Detalhar	Estatísticas de leitura/gravação de baixo nível e por protocolo para todos os objetos rastreados: • Nós • Agregados • LUNs • Volumes • Discos • LIFs • Portas/NICs	Este grupo fornece detalhamentos 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, tanto o objeto antigo quanto o novo conterão dados de desempenho no servidor externo (chamado de “metric_path”). Os dois objetos não estão correlacionados como o mesmo objeto. Por exemplo, se você alterar o nome de um volume de “volume1_acct” para “acct_vol1”, 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 Conhecimento para obter a lista de todos os contadores de desempenho que podem ser enviados a um provedor de dados externo.

["Contadores de desempenho do Unified Manager que podem ser exportados para um Provedor de Dados Externo"](#)

Configurar o Graphite para receber dados de desempenho do Unified Manager

Graphite é uma ferramenta de software aberta para coletar e representar graficamente dados de desempenho de sistemas de computador. Seu servidor e software Graphite devem estar configurados corretamente para receber dados estatísticos do Unified Manager.

A NetApp não testa nem 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 dar suporte à 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 na sua configuração e dos objetos de estatísticas que você selecionou para enviar, pode haver milhares de novos arquivos que precisam ser criados inicialmente. Com 200 arquivos por minuto, pode levar 15 minutos ou mais para que todos os arquivos de métricas sejam criados inicialmente. Depois que todos os arquivos de métricas exclusivos forem criados, esse

parâmetro não será 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` o arquivo deve ser alterado de “0.0.0.0” para “::”(`LINE_RECEIVER_INTERFACE = ::`)
- No `/opt/graphite/conf/storage-schemas.conf` arquivo, o `retentions` O parâmetro deve ser usado para definir a frequência para 5 minutos e o período de retenção para o número de dias relevante para seu ambiente.

O período de retenção pode ser tão longo quanto o seu ambiente permitir, mas o valor de frequência deve ser definido como 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 do fornecedor padrão for alterada de “netapp-performance” para algo diferente, essa alteração deve ser refletida no `pattern` parâmetro também.



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.

Configurar 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 em que os dados são enviados.

Antes de começar

- Você deve ter uma ID de usuário autorizada para efetuar 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:
 - `INDICADOR_DE_PERFORMANCE`: Estatísticas do monitor de desempenho
 - `RESOURCE_UTILIZATION`: Estatísticas de utilização de recursos e monitor de desempenho
 - `DRILL_DOWN`: Todas as estatísticas
- Você deve saber o intervalo de tempo em que deseja transmitir estatísticas: 5, 10 ou 15 minutos

Por padrão, o Unified Manager coleta estatísticas em intervalos de 5 minutos. Se você definir o intervalo

de transmissão para 10 (ou 15) minutos, a quantidade de dados enviados durante cada transmissão será duas (ou três) vezes maior do que quando usar o intervalo padrão de 5 minutos.



Se você alterar o intervalo de coleta de desempenho do Unified Manager para 10 ou 15 minutos, deverá alterar o intervalo de transmissão para que 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. Efetue 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 **Provedor de Dados Externo**.

O menu Conexão de servidor externo é exibido.

3. Digite o número da opção de menu **Adicionar/Modificar conexão do servidor**.

As informações atuais de conexão do servidor 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 de servidor externo.

8. Digite o número da opção de menu **Modificar configuração do servidor**.

As informações atuais de configuração do servidor são exibidas.

9. Quando solicitado, digite **y** para continuar.

10. Quando solicitado, insira o tipo de estatísticas a serem enviadas, o intervalo de tempo em que as estatísticas são enviadas e se deseja habilitar a transmissão de estatísticas agora:

Para..	Digitar...
ID do grupo de estatísticas	0- INDICADOR_DE_DESEMPENHO (padrão) 1- UTILIZAÇÃO_DE_RECURSOS 2- DETALHE

Para..	Digitar...
Etiqueta do fornecedor	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. Usando a notação pontilhada, você pode definir uma estrutura de pastas hierárquica. Por exemplo, ao inserir stats.performance.netapp as estatísticas estarão localizadas em stats > performance > netapp.
Intervalo de transmissão	5(padão), 10 , ou 15 minutos
Habilitar/desabilitar	0- Desabilitar 1- Habilitar (padrão)

11. Quando solicitado, digite **y** para verificar se as informações inseridas estão corretas.
12. Pressione qualquer tecla para retornar ao menu Conexão de servidor externo.
13. Tipo **x** para sair do console de manutenção.

Depois de configurar a conexão, os dados de desempenho selecionados são enviados ao servidor de destino no intervalo de tempo especificado. Demora alguns minutos até que as métricas comecem a aparecer na ferramenta externa. Talvez seja necessário atualizar seu navegador para ver as novas métricas na hierarquia de métricas.

Monitorar e gerenciar a integridade do cluster

Introdução ao monitoramento de integridade do Active IQ Unified Manager

O Active IQ Unified Manager (antigo OnCommand Unified Manager) ajuda você a monitorar um grande número de sistemas que executam o software ONTAP por meio de uma interface de usuário centralizada. A infraestrutura do servidor do Unified Manager oferece escalabilidade, capacidade de suporte e recursos aprimorados de monitoramento e notificação.

Os principais recursos do Unified Manager incluem monitoramento, alertas, gerenciamento de disponibilidade e capacidade de clusters, gerenciamento de recursos de proteção e agrupamento de dados de diagnóstico e envio para suporte técnico.

Você pode usar o Unified Manager para monitorar seus clusters. Quando ocorrem problemas no cluster, o Unified Manager notifica você sobre os detalhes desses 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 ocorrerem problemas, você seja notificado por e-mail e traps SNMP.

Você pode usar o Unified Manager para gerenciar objetos de armazenamento 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 seus objetos de cluster usando as informações fornecidas nos gráficos de capacidade e integridade do respectivo objeto de cluster.

Capacidade física e lógica

O Unified Manager utiliza os conceitos de espaço físico e lógico usados para objetos de armazenamento ONTAP .

- Capacidade física: Espaço físico refere-se aos blocos físicos de armazenamento usados no volume. A “capacidade física utilizada” é normalmente menor que a capacidade lógica utilizada devido à redução de dados devido a recursos de eficiência de armazenamento (como deduplicação e compactação).
- Capacidade lógica: Espaço lógico refere-se ao espaço utilizável (os blocos lógicos) em um volume. Espaço lógico refere-se a como o espaço teórico pode ser usado, sem levar em conta os resultados de deduplicação ou compactação. “Espaço lógico usado” é o espaço físico usado mais a economia dos recursos de eficiência de armazenamento (como deduplicação e compactação) que foram configurados. Essa medição geralmente parece maior que a capacidade física utilizada porque não reflete a compactação de dados e outras reduções no espaço físico. Assim, a capacidade lógica total pode ser maior que o espaço provisionado.

Unidades de medida de 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 versões anteriores, essas unidades eram exibidas como KB, MB, GB, TB e PB. A partir do ONTAP 9.10.1, eles são exibidos no Unified Manager como KiB, MiB, GiB, TiB e PiB.



As unidades usadas para taxa de transferência continuam sendo quilobytes 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 Unified Manager para ONTAP 9.10.0 e versões anteriores	Unidade de capacidade exibida no Unified Manager para 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
tuberculose	TiB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 bytes

Recursos de monitoramento de integridade do Unified Manager

O Unified Manager é criado em uma infraestrutura de servidor que oferece escalabilidade, capacidade de suporte e recursos aprimorados de monitoramento e notificação. O Unified Manager oferece suporte ao monitoramento de sistemas que executam o software ONTAP .

O Unified Manager inclui os seguintes recursos:

- Descoberta, monitoramento e notificações para sistemas instalados com software ONTAP :
 - Objetos físicos: nós, discos, prateleiras de disco, pares SFO, portas e Flash Cache
 - Objetos lógicos: clusters, máquinas virtuais de armazenamento (SVMs), agregados, volumes, LUNs, namespaces, qtrees, LIFs, cópias de instantâneos, 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 armazenamento: agregados SSD, agregados Flash Pool, agregados FabricPool , deduplicação e compactação
 - Proteção: relacionamentos SnapMirror (síncronos e assíncronos) e relacionamentos SnapVault
- Visualizando o status de descoberta e monitoramento do cluster
- MetroCluster sobre configurações de FC e IP: visualização e monitoramento da configuração, problemas e status de conectividade dos componentes do cluster. Switches e pontes MetroCluster para configurações MetroCluster sobre FC
- Alertas, eventos e infraestrutura de limite aprimorados
- Autenticação LDAP, LDAPS, SAML e suporte ao usuário local
- RBAC (para um conjunto predefinido de funções)

- Pacote de suporte e suporte AutoSupport
- Painel aprimorado para mostrar capacidade, disponibilidade, proteção e desempenho do ambiente
- Interoperabilidade de movimentação de volume, histórico de movimentação de volume e histórico de alterações de caminho de junção
- Área de escopo de impacto que exibe graficamente os recursos afetados por eventos como Alguns discos com falha, Espelhamento agregado do MetroCluster degradado e Discos sobressalentes do MetroCluster deixados para trás
- Área de efeito possível que exibe o efeito dos eventos do MetroCluster
- Área de Ações Corretivas Sugeridas que exibe as ações que podem ser executadas para resolver eventos como Alguns Discos com Falha, Espelhamento de Agregação do MetroCluster Degradado e Discos Sobressalentes do MetroCluster Deixados para Trás
- Área de recursos que podem ser impactados que exibe os recursos que podem ser impactados por eventos como o evento Volume Offline, o evento Volume Restrito e o evento Espaço de Volume Thin-Provisioned em Risco
- Suporte para SVMs com volumes FlexVol ou FlexGroup
- Suporte para monitoramento de volumes raiz de nós
- Monitoramento aprimorado de cópias de Snapshot, incluindo computação de espaço recuperável e exclusão de cópias de Snapshot
- Anotações para objetos de armazenamento
- Criação de relatórios e gerenciamento de informações de objetos de armazenamento, como capacidade física e lógica, utilização, economia de espaço, desempenho e eventos relacionados
- Integração com OnCommand Workflow Automation para executar fluxos de trabalho

O Storage Automation Store contém pacotes de fluxo de trabalho de armazenamento automatizado certificados pela NetApp, desenvolvidos para uso com o OnCommand Workflow Automation (WFA). Você pode baixar os pacotes e importá-los para o WFA para executá-los. Os fluxos de trabalho automatizados estão disponíveis aqui:

["Loja de automação de armazenamento"](#)

Interfaces do Unified Manager usadas para gerenciar a integridade do sistema de armazenamento

Estas seções contêm informações sobre as duas interfaces de usuário que o Active IQ Unified Manager fornece para solucionar problemas de capacidade de armazenamento de dados, disponibilidade e proteção. As duas interfaces de usuário são a interface de usuário da Web do Unified Manager e o console de manutenção.

Se quiser usar os recursos de proteção no Unified Manager, você também deve instalar e configurar o OnCommand Workflow Automation (WFA).

Interface da Web do Unified Manager

A interface de usuário da Web do Unified Manager permite que um administrador monitore e solucione problemas de cluster relacionados à capacidade de armazenamento de dados, disponibilidade e proteção.

Estas seções descrevem alguns fluxos de trabalho comuns que um administrador pode seguir para solucionar

problemas de capacidade de armazenamento, disponibilidade de dados ou proteção exibidos na interface do usuário da Web do Unified Manager.

Console de manutenção

O console de manutenção do Unified Manager permite que um administrador monitore, diagnostique e resolva 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 interface de usuário 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-las para resolver problemas relacionados ao funcionamento do servidor do Unified Manager.

Gerenciando e monitorando clusters e integridade de objetos de 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 quaisquer riscos de disponibilidade e capacidade.

Entenda o monitoramento de cluster

Você pode adicionar clusters ao banco de dados do Unified Manager para monitorar clusters quanto à disponibilidade, capacidade e outros detalhes, como uso da CPU, estatísticas de interface, espaço livre em disco, uso do qtree e ambiente do chassi.

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 a um destinatário especificado quando um evento aciona um alerta.

Entenda os volumes raiz do nó

Você pode monitorar o volume raiz do nó usando o Unified Manager. A melhor prática é que o volume raiz do nó tenha capacidade suficiente para evitar que o nó fique inativo.

Quando a capacidade utilizada do volume raiz do nó excede 80% da capacidade total do volume raiz do nó, o evento Espaço de volume raiz do nó quase cheio é gerado. Você pode configurar um alerta para o evento para receber uma notificação. Você pode tomar as medidas apropriadas para evitar que o nó fique inativo usando o ONTAP System Manager ou o ONTAP CLI.



A funcionalidade de monitoramento de volumes raiz de nós não estará disponível se os clusters executarem o ONTAP versão 9.14.1 ou posterior.

Entenda eventos e limites para agregados de raiz de nó

Você pode monitorar o agregado raiz do nó usando o Unified Manager. A melhor prática é provisionar densamente o volume raiz no agregado raiz para evitar que o nó pare.

Por padrão, eventos de capacidade e desempenho não são gerados para agregados raiz. Além disso, os valores limite usados pelo Unified Manager não são aplicáveis aos agregados raiz do nó. Somente um representante de suporte técnico pode modificar as configurações para que esses eventos sejam gerados. Quando as configurações são modificadas pelo representante de suporte técnico, os valores de limite de capacidade são aplicados ao agregado raiz do nó.

Você pode tomar as medidas apropriadas para evitar que o nó pare usando o ONTAP System Manager ou o ONTAP CLI.



A funcionalidade de monitoramento de agregados raiz de nós não estará disponível se os clusters executarem o ONTAP versão 9.14.1 ou posterior.

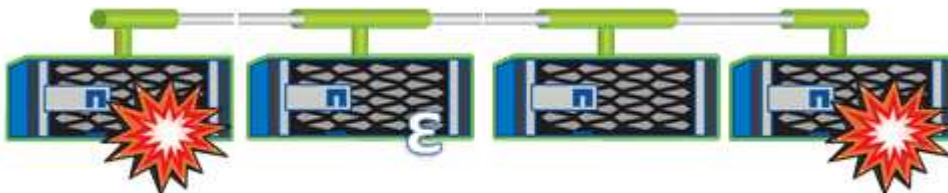
Entenda o quorum e o epsilon

Quorum e epsilon são medidas importantes da saúde e função do cluster que, juntas, 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 em quorum, uma maioria simples de nós está saudável e pode se comunicar entre si. Quando o quorum é perdido, o cluster perde a capacidade de realizar operações normais de cluster. Somente uma coleção de nós pode ter quorum por vez, porque todos os nós compartilham coletivamente uma única visão dos dados. Portanto, se dois nós não comunicantes tiverem permissão para 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 mestre é responsável por sincronizar informações em todo o cluster. Quando o quórum é formado, ele é mantido por votação contínua. Se o nó mestre ficar offline e o cluster ainda estiver no quorum, um novo mestre será eleito pelos nós que permanecerem online.

Como há a possibilidade de empate em um cluster que tem um número par de nós, um nó tem um peso de votação fracionário extra chamado *épsilon*. Se a conectividade entre duas porções iguais de um grande cluster falhar, o grupo de nós que contém epsilon mantém o quorum, 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. Entretanto, como um dos nós sobreviventes contém epsilon, o cluster permanece no quorum mesmo que 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 contém o epsilon ficar com problemas, assumir o controle de seu parceiro de alta disponibilidade ou for assumido por seu parceiro de alta disponibilidade, o epsilon será automaticamente reatribuído a um nó saudável em um par de HA diferente.

Colocar um nó offline pode afetar a capacidade do cluster de permanecer no quorum. Portanto, o ONTAP emite uma mensagem de aviso se você tentar uma operação que tire o cluster do quorum ou o coloque a uma indisponibilidade de uma perda de quorum. Você pode desabilitar as mensagens de aviso de quorum usando o comando `cluster quorum-service options modify` no nível de privilégio avançado.

Em geral, assumindo conectividade confiável entre os nós do cluster, um cluster maior é mais estável que um cluster menor. O requisito de quorum de uma maioria simples de metade dos nós mais 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 específicos para manter o quorum. Clusters de dois nós usam HA de cluster, no qual nenhum nó contém epsilon; em vez disso, ambos os nós são continuamente pesquisados para garantir que, se um nó falhar, o outro tenha acesso total de leitura e gravação aos dados, bem como acesso a interfaces lógicas e funções de gerenciamento.

Veja a lista de clusters e detalhes

Você pode usar a visualização Saúde: Todos os clusters para visualizar seu inventário de clusters. A exibição Capacidade: Todos os clusters permite que você visualize informações resumidas sobre a capacidade de armazenamento e utilização em todos os clusters.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Você também pode visualizar detalhes de clusters individuais, como integridade, capacidade, configuração, LIFs, nós e discos naquele cluster, usando a página Detalhes do cluster/integridade.

Os detalhes na visualização Integridade: Todos os clusters, Capacidade: Todos os clusters e a página Detalhes do cluster/integridade ajudam você a planejar seu armazenamento. 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 **Armazenamento > Clusters**.
2. No menu Exibir, selecione a exibição **Saúde: Todos os clusters** para visualizar informações de integridade ou a exibição **Capacidade: Todos os clusters** para visualizar detalhes sobre a capacidade de armazenamento e utilização em todos os clusters.
3. Clique no nome de um cluster para visualizar detalhes completos do cluster na página de detalhes **Cluster / Saúde**.

Informações relacionadas

- ["Página de detalhes do cluster/saúde"](#)
- ["Desempenho: visualização de todos os clusters"](#)
- ["Monitoramento das configurações do MetroCluster"](#)
- ["Visualizando o status de segurança de clusters e VMs de armazenamento"](#)
- ["Quais critérios de segurança estão sendo avaliados"](#)

Verifique a integridade dos clusters em uma configuração MetroCluster

Você pode usar o Active IQ Unified Manager (Unified Manager) para verificar a integridade operacional dos clusters e seus componentes nas configurações do MetroCluster sobre FC e do MetroCluster sobre IP. Se os clusters estiverem envolvidos em um evento de desempenho detectado pelo Unified Manager, o status de integridade

pode ajudar a determinar se um problema de hardware ou software contribuiu para o evento.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos 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 sobre FC e IP devem ser monitorados pela mesma instância do Unified Manager.

Determinar a integridade do cluster no MetroCluster por meio da configuração FC

Siga estas etapas para determinar a integridade do cluster em uma configuração MetroCluster sobre FC.

Passos

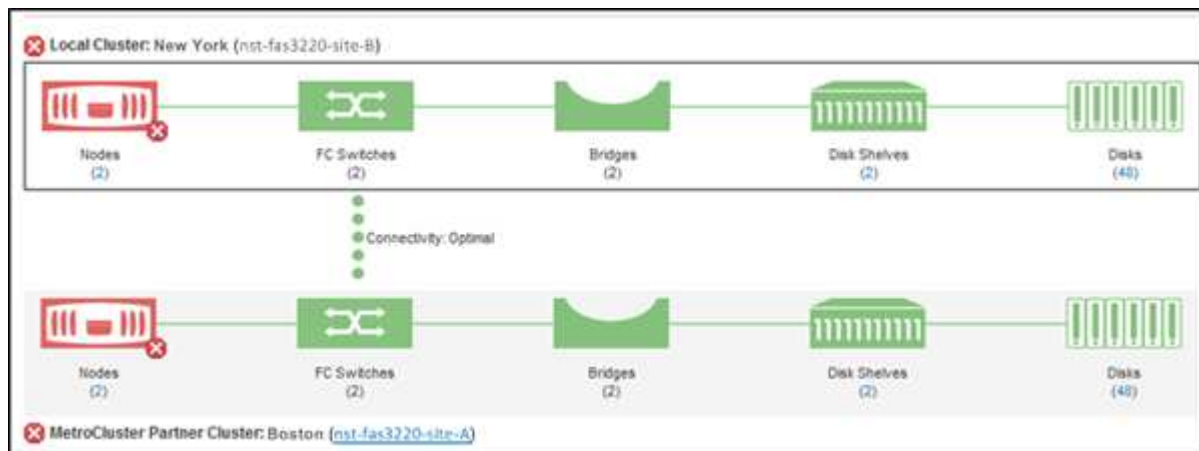
1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos** para exibir a lista de eventos.
2. No painel de filtros, selecione todos os filtros do MetroCluster na categoria **Tipo de fonte**. Você vê todos os eventos gerados no seu ambiente para todas as configurações do MetroCluster .
3. Ao lado de um evento do MetroCluster , clique no nome do cluster.



Se nenhum evento do MetroCluster for exibido, você pode usar a barra de pesquisa para procurar o nome do cluster envolvido no evento relacionado à sua configuração do MetroCluster sobre FC.

A visualização Saúde: Todos os clusters é exibida com informações detalhadas sobre o evento.

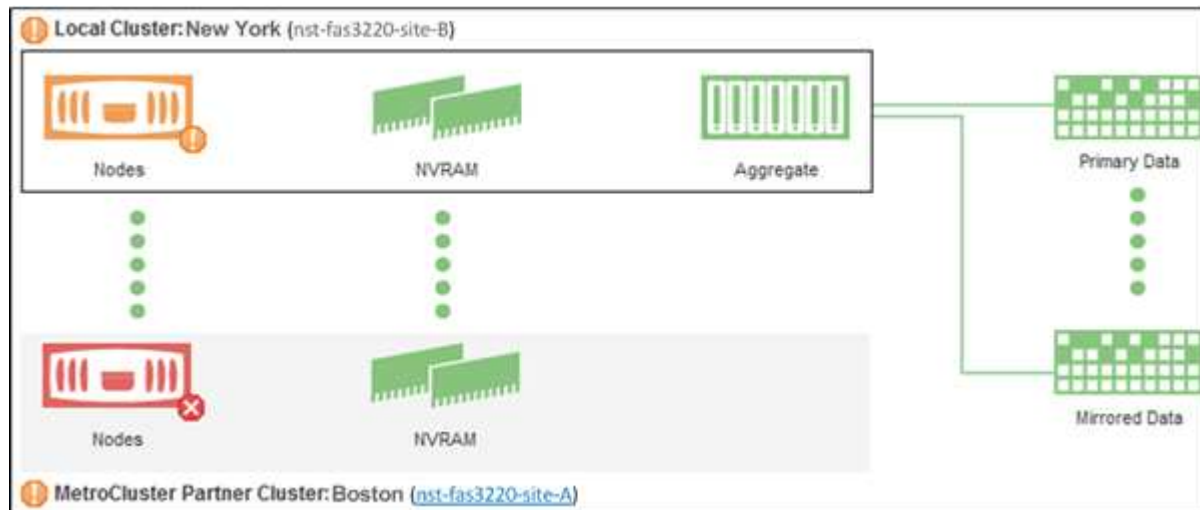
4. Selecione a aba * Conectividade do MetroCluster * para exibir a integridade da conexão entre o cluster selecionado e seu cluster parceiro.



Neste exemplo, os nomes e os componentes do cluster local e seu cluster parceiro são exibidos. Um ícone amarelo ou vermelho indica um evento de integridade para o componente destacado. O ícone Conectividade representa o link entre os clusters. Você pode apontar o cursor do mouse para um ícone para exibir informações do evento ou clicar no ícone para exibir os eventos. Um problema de saúde em qualquer um dos clusters pode ter contribuído para o evento de desempenho.

O Unified Manager monitora o componente NVRAM do link entre os clusters. Se o ícone FC Switches no cluster local ou de parceiro ou o ícone Conectividade estiver vermelho, um problema de integridade do link pode ter causado o evento de desempenho.

5. Selecione a aba * MetroCluster Replication*.



Neste exemplo, se o ícone da NVRAM no cluster local ou parceiro estiver amarelo ou vermelho, um problema de integridade com a 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.

Determinar a integridade do cluster na configuração do 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 gerados no seu ambiente para todas as configurações do MetroCluster .



Se você não conseguir ver os eventos relatados do MetroCluster , poderá usar a barra de pesquisa para pesquisar pelo nome do cluster envolvido no evento relacionado à sua configuração do 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, consulte "[Monitorar problemas de conectividade na configuração do MetroCluster sobre IP](#)" .

Visualizar o status de integridade e capacidade de todos os clusters do SAN Array

Você pode usar as páginas de inventário do Cluster para exibir o status de integridade e capacidade dos seus clusters All SAN Array.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode visualizar informações gerais para todos os clusters do SAN Array na exibição Saúde: Todos os clusters e Capacidade: Todos os clusters. Além disso, você pode visualizar detalhes na página Detalhes do Cluster/Saúde.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Clusters**.
2. Certifique-se de que a coluna “Personalidade” seja exibida na exibição **Saúde: Todos os Clusters** ou adicione-a usando o controle **Mostrar / Ocultar**.

Esta coluna exibe “All SAN Array” para seus clusters All SAN Array.

3. Revise as informações.
4. Para visualizar informações sobre a capacidade de armazenamento nesses clusters, selecione a exibição **Capacidade: Todos os clusters**.
5. Para visualizar informações detalhadas sobre a integridade e a capacidade de armazenamento nesses clusters, clique no nome de um cluster All SAN Array.

Visualize os detalhes nas guias Saúde, Capacidade e Nós na página Detalhes do cluster/saúde

Ver a lista de nós e detalhes

Você pode usar a visualização Saúde: Todos os nós para visualizar a lista de nós em seus clusters. Você pode usar a página Detalhes do cluster/integridade para visualizar informações detalhadas sobre os nós que fazem parte do cluster monitorado.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode visualizar detalhes como o estado do nó, o cluster que contém o nó, detalhes da capacidade agregada (usada e total) e detalhes da capacidade bruta (utilizável, sobressalente e total). Você também pode obter informações sobre pares de HA, prateleiras de discos e portas.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Nós**.
2. Na visualização **Saúde: Todos os nós**, clique no nó cujos detalhes você deseja visualizar.

As informações detalhadas do nó selecionado são exibidas na página Detalhes do cluster/integridade. O painel esquerdo exibe a lista de pares de HA. Por padrão, os Detalhes do HA estão abertos, exibindo detalhes do estado do HA e eventos relacionados ao par de HA selecionado.

3. Para visualizar outros detalhes sobre o nó, execute a ação apropriada:

Para visualizar...	Clique...
Detalhes sobre as prateleiras de disco	Prateleiras de disco.
Informações relacionadas ao porto	Portas.

Para mais informações, consulte:

- ["Desempenho: visualização de todos os nós"](#)
- ["Visualizando valores de IOPS disponíveis de nós e agregados"](#)

- "Visualizando valores usados de capacidade de desempenho de nós e agregados"

Gerar um relatório de inventário de hardware para renovação de contrato

Você pode gerar um relatório que contém uma lista completa de informações do cluster e do 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 renovação de contratos em sites seguros (sites *escuros*) que não estão conectados à plataforma NetAppActive IQ.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Nós**.
2. Acesse 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 da data atual.

4. Forneça essas informações ao seu contato de suporte da NetApp para renovação do contrato.

Veja a lista e os detalhes da VM de armazenamento

Na exibição Saúde: todas as VMs de armazenamento, você pode monitorar seu inventário de máquinas virtuais de armazenamento (SVMs). Você pode usar a página Detalhes da VM de armazenamento/Integridade para visualizar informações detalhadas sobre as SVMs monitoradas.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode visualizar detalhes do SVM, como capacidade, eficiência e configuração de um SVM. Você também pode visualizar informações sobre os dispositivos relacionados e alertas relacionados para esse SVM.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > VMs de armazenamento**.
2. Escolha uma das seguintes maneiras de visualizar os detalhes do SVM:
 - Para visualizar informações sobre a integridade de todas as SVMs em todos os clusters, no menu Exibir, selecione Integridade: visualização Todas as VMs de armazenamento.
 - Para visualizar 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 de detalhes mínimos.

3. Visualize os objetos relacionados ao SVM clicando em **Visualizar relacionados** na caixa de diálogo de detalhes mínimos.

Informações relacionadas

- ["VM de armazenamento: página de detalhes de integridade"](#)
- ["Desempenho: visualização de todas as VMs de armazenamento"](#)
- ["Segurança: Visão anti-ransomware"](#)
- ["Visualizando o status de segurança de clusters e VMs de armazenamento"](#)
- ["Relacionamento: Visualização de todos os relacionamentos"](#)

Veja a lista agregada e os detalhes

Na visualização Saúde: Todos os agregados, você pode monitorar seu inventário de agregados. A exibição Capacidade: Todos os agregados permite que você visualize informações sobre a capacidade e a utilização de agregados em todos os clusters.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode visualizar detalhes como capacidade e configuração agregadas e informações do disco na página Detalhes do agregado/saúde. Você pode usar esses detalhes antes de configurar as configurações de limite, se necessário.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Agregados**.
2. Escolha uma das seguintes maneiras de visualizar os detalhes agregados:
 - Para visualizar informações sobre a integridade de todos os agregados em todos os clusters, no menu Exibir, selecione Integridade: visualização Todos os agregados.
 - Para visualizar informações sobre a capacidade e a utilização de todos os agregados em todos os clusters, no menu Exibir, selecione Capacidade: visualização 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 de detalhes mínimos.

3. Visualize os objetos relacionados ao agregado clicando em **Visualizar relacionados** na caixa de diálogo de detalhes mínimos.

Informações relacionadas

- ["Página de detalhes agregados/de saúde"](#)
- ["Desempenho: Visualização de todos os agregados"](#)
- ["Personalizando relatórios de capacidade agregada"](#)

Ver informações sobre a capacidade do FabricPool

Você pode visualizar informações de capacidade do FabricPool para clusters, agregados e volumes nas páginas de detalhes e inventário de Capacidade e Desempenho desses objetos. Essas páginas também exibem informações do espelho do FabricPool quando uma camada de espelho foi configurada.

Essas páginas exibem informações como a capacidade disponível na camada de desempenho 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 determinadas informações para a camada de nuvem.

Quando uma camada de nuvem é espelhada para outro provedor de nuvem (a “camada de espelho”), ambas as camadas de nuvem são exibidas na página Detalhes agregados/saúde.

Passos

1. Execute um dos seguintes procedimentos:

Para visualizar informações de capacidade para...	Faça isso...
Aglomerados	a. Na exibição Capacidade: Todos os clusters, clique em um cluster. b. Na página Detalhes do Cluster/Saúde, clique na guia Configuração. A exibição mostra os nomes de todas as camadas de nuvem às quais este cluster está conectado.
Agregados	a. Na exibição Capacidade: Todos os agregados, clique em um agregado em que o campo Tipo indique “SSD (FabricPool)” ou “HDD (FabricPool)”. b. Na página Detalhes agregados/saúde, clique na guia Capacidade. O visor mostra a capacidade total usada na camada de nuvem. c. Clique na aba Informações do disco. A exibição mostra o nome do nível da nuvem e a capacidade utilizada. d. Clique na aba Configuração. A exibição mostra o nome da camada de nuvem e outras informações detalhadas sobre a camada de nuvem.

Para visualizar informações de capacidade para...	Faça isso...
Volumes	a. Na exibição Capacidade: Todos os volumes, clique em um volume onde um nome de política apareça no campo “Política de camadas”. b. Na página Detalhes do volume/saúde, clique na guia Configuração. A exibição mostra o nome da política de camadas do FabricPool atribuída ao volume.

- Na página **Análise de carga de trabalho**, você pode selecionar “Visualização 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 , consulte ["Visão geral de discos e agregados"](#) .

Ver detalhes do pool de armazenamento

Você pode visualizar os detalhes do pool de armazenamento para monitorar a integridade do pool de armazenamento, o cache total e disponível e as alocações usadas e disponíveis.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

- No painel de navegação esquerdo, clique em **Armazenamento > Agregados**.
- Clique em um nome agregado.

Os detalhes do agregado selecionado são exibidos.

- Clique na aba **Informações do disco**.

Informações detalhadas do disco são exibidas.



A tabela Cache é exibida somente quando o agregado selecionado está 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.

Veja a lista de volumes e detalhes

Na visualização Saúde: Todos os volumes, você pode monitorar seu inventário de volumes. A exibição Capacidade: Todos os volumes permite que você visualize informações sobre a capacidade e a utilização de volumes em um cluster.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Você também pode usar a página Detalhes do volume/saúde para visualizar informações detalhadas sobre os volumes monitorados, incluindo capacidade, eficiência, configuração e proteção dos volumes. Você também pode visualizar informações sobre os dispositivos relacionados e alertas relacionados para um volume específico.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. Escolha uma das seguintes maneiras de visualizar os detalhes do volume:
 - Para visualizar informações detalhadas sobre a integridade dos volumes em um cluster, no menu Exibir, selecione Integridade: visualização Todos os volumes.
 - Para visualizar informações detalhadas sobre a capacidade e a utilização de volumes em um cluster, no menu Exibir, selecione Capacidade: visualização 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 de detalhes mínimos.
3. **Opcional:** visualize os objetos relacionados ao volume clicando em **Exibir relacionados** na caixa de diálogo de detalhes mínimos.

Informações relacionadas

- ["Volume: Página de detalhes de saúde"](#)
- ["Desempenho: Visualização de todos os volumes"](#)
- ["Segurança: Visão anti-ransomware"](#)
- ["Visualizando relacionamentos de proteção de volume"](#)
- ["Criação de um relatório para visualizar gráficos de capacidade de volume disponíveis"](#)

Ver detalhes sobre ações NFS

Você pode visualizar detalhes sobre todos os compartilhamentos NFS, como seu status, o caminho associado ao volume (volumes FlexGroup ou FlexVol), níveis de acesso de clientes aos compartilhamentos NFS e a política de exportação definida para os volumes exportados. Use a exibição Integridade: Todos os compartilhamentos NFS para ver todos os compartilhamentos NFS em todos os clusters monitorados e use a página de detalhes da VM de armazenamento/Integridade para visualizar todos os compartilhamentos NFS em uma máquina virtual de armazenamento (SVM) específica.

Antes de começar

- A licença NFS deve estar habilitada no cluster.
- As interfaces de rede que atendem aos compartilhamentos NFS devem ser configuradas.
- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Etapa

1. No painel de navegação esquerdo, siga as etapas abaixo, dependendo se você deseja visualizar todos os compartilhamentos NFS ou apenas os compartilhamentos NFS de um SVM específico.

Para...	Siga estes passos...
Ver todas as ações do NFS	Clique em Armazenamento > Compartilhamentos NFS
Exibir compartilhamentos NFS para SVM único	a. Clique em Armazenamento > VMs de armazenamento b. Clique no SVM cujos detalhes dos compartilhamentos NFS você deseja visualizar. c. Na página Detalhes da VM de armazenamento/integridade, clique na guia Compartilhamentos NFS.

Para mais informações, consulte ["Provisionando volumes de compartilhamento de arquivos"](#) e ["Provisionamento de compartilhamentos de arquivos CIFS e NFS usando APIs"](#).

Ver detalhes sobre ações SMB/CIFS

Você pode visualizar detalhes sobre todos os compartilhamentos SMB/CIFS, como nome do compartilhamento, caminho de junção, objetos contidos, configurações de segurança e políticas de exportação definidas para o compartilhamento. Use a exibição Integridade: todos os compartilhamentos SMB para ver todos os compartilhamentos SMB em todos os clusters monitorados e use a página de detalhes da VM de armazenamento/Integridade para visualizar todos os compartilhamentos SMB em uma máquina virtual de armazenamento (SVM) específica.

Antes de começar

- A licença CIFS deve estar habilitada no cluster.
- As interfaces de rede que atendem aos compartilhamentos SMB/CIFS devem ser configuradas.
- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.



Compartilhamentos em pastas não são exibidos.

Etapa

1. No painel de navegação esquerdo, siga as etapas abaixo, dependendo se você deseja visualizar todos os compartilhamentos SMB/CIFS ou apenas os compartilhamentos de um SVM específico.

Para...	Siga estes passos...
Ver todas as ações SMB/CIFS	Clique em Armazenamento > Compartilhamentos SMB

Para...	Siga estes passos...
Exibir compartilhamentos SMB/CIFS para SVM único	- Clique em Armazenamento > VMs de armazenamento - Clique no SVM cujos detalhes do compartilhamento SMB/CIFS você deseja visualizar. - Na página Detalhes da VM de armazenamento/integridade, clique na guia Compartilhamentos SMB.

Para mais informações, consulte ["Provisionamento de compartilhamentos de arquivos CIFS e NFS usando APIs"](#).

Veja a lista de cópias do Snapshot

Você pode visualizar a lista de cópias do Snapshot para um volume selecionado. Você pode usar a lista de cópias do Snapshot para calcular a quantidade de espaço em disco que pode ser recuperada se uma ou mais cópias do Snapshot forem excluídas. Você pode excluir as cópias do Snapshot, se necessário.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- O volume contendo as cópias do Snapshot deve estar online.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. Na exibição **Saúde: Todos os volumes**, selecione o volume que contém as cópias do Snapshot que você deseja visualizar.
3. Na página de detalhes **Volume / Saúde**, clique na aba **Capacidade**.
4. No painel **Detalhes** da guia **Capacidade**, na seção Outros detalhes, clique no link ao lado de **Cópias instantâneas**.

O número de cópias do Snapshot é um link que exibe a lista de cópias do Snapshot.

Informações relacionadas

["Página de Saúde/Volumes"](#)

Excluir cópias do Snapshot

Você pode excluir uma cópia do Snapshot para economizar espaço ou liberar espaço em disco, ou pode excluir a cópia do Snapshot se ela não for mais necessária.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

O volume deve estar online.

Para excluir uma cópia do Snapshot que está ocupada ou bloqueada, você deve ter liberado a cópia do Snapshot do aplicativo que a estava usando.

- Não é possível excluir a cópia base do Snapshot em um volume pai se um volume FlexClone estiver usando essa cópia do Snapshot.

A cópia base do Snapshot é a cópia do Snapshot usada para criar o volume FlexClone e exibe o status `Busy` e Dependência de Aplicação como `Busy`, `Vclone` no volume pai.

- Não é possível excluir uma cópia bloqueada do Snapshot que é usada em um relacionamento SnapMirror .

A cópia do Snapshot está bloqueada e é necessária para a próxima atualização.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. Na exibição **Saúde: Todos os volumes**, selecione o volume que contém as cópias do Snapshot que você deseja visualizar.

A lista de cópias do Snapshot é exibida.

3. Na página de detalhes **Volume / Saúde**, clique na aba **Capacidade**.
4. No painel **Detalhes** da guia **Capacidade**, na seção Outros detalhes, clique no link ao lado de **Cópias instantâneas**.

O número de cópias do Snapshot é um link que exibe a lista de cópias do Snapshot.

5. Na visualização **Cópias de instantâneo**, selecione as cópias de instantâneo que deseja excluir e clique em **Excluir selecionadas**.

Calcular espaço recuperável para cópias de Snapshot

Você pode calcular a quantidade de espaço em disco que pode ser recuperada se uma ou mais cópias do Snapshot forem excluídas.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- O volume deve estar online.
- O volume deve ser um FlexVol volume; esse recurso não é suportado com volumes FlexGroup .

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. Na exibição **Saúde: Todos os volumes**, selecione o volume que contém as cópias do Snapshot que você deseja visualizar.

A lista de cópias do Snapshot é exibida.

3. Na página de detalhes **Volume / Saúde**, clique na aba **Capacidade**.
4. No painel **Detalhes** da guia **Capacidade**, na seção Outros detalhes, clique no link ao lado de **Cópias instantâneas**.

O número de cópias do Snapshot é um link que exibe a lista de cópias do Snapshot.

5. Na exibição **Cópias de instantâneo**, selecione as cópias de instantâneo para as quais você deseja calcular o espaço recuperável.
6. Clique em **Calcular**.

O espaço recuperável (em porcentagem, KB, MB, GB e assim por diante) no volume é exibido.

7. Para recalcular o espaço recuperável, selecione as cópias do Snapshot necessárias e clique em **Recalcular**.

Descrição das janelas e caixas de diálogo de objetos de cluster

Você pode visualizar todos os seus clusters e objetos de cluster na respectiva página de objeto de armazenamento. 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 ARMAZENAMENTO e PROTEÇÃO do INVENTÁRIO.

- Páginas de inventário de cluster, integridade do cluster e desempenho do cluster
- Páginas de Inventário Agregado, Saúde Agregada e Desempenho Agregado
- Páginas de Inventário de Volume, Saúde do Volume e Desempenho do Volume
- 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

Fluxos de trabalho e tarefas comuns de saúde do Unified Manager

Alguns fluxos de trabalho e tarefas administrativas comuns associados ao Unified Manager incluem selecionar os clusters de armazenamento que devem ser monitorados; diagnosticar condições que afetam negativamente a disponibilidade, a capacidade e a proteção dos dados; restaurar dados perdidos; configurar e gerenciar volumes; e agrupar e enviar dados de diagnóstico ao suporte técnico (quando necessário).

O Unified Manager permite que os administradores de armazenamento visualizem um painel, avaliem a capacidade geral, a disponibilidade e a integridade da proteção dos clusters de armazenamento gerenciados e, em seguida, identifiquem, localizem, diagnostiquem e atribuam rapidamente para resolução quaisquer 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 dos seus objetos de armazenamento gerenciados são exibidos nos gráficos de integridade do sistema e eventos na página Painel. Quando problemas críticos são identificados, esta página fornece links para dar suporte a 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 dar suporte à

configuração direta de recursos de armazenamento.

Fluxos de trabalho comuns relacionados às seguintes tarefas administrativas são descritos neste documento:

- Diagnosticar e gerenciar problemas de disponibilidade

Se falhas de hardware ou problemas de configuração de recursos de armazenamento causarem a exibição de eventos de disponibilidade de dados na página Painel, os administradores de armazenamento poderão seguir os links incorporados para visualizar informações de conectividade sobre o recurso de armazenamento afetado, visualizar conselhos sobre solução de problemas e atribuir a resolução de problemas a outros administradores.

- Configurando e monitorando incidentes de desempenho

O administrador pode monitorar e gerenciar o desempenho dos recursos do sistema de armazenamento que estão sendo monitorados. Veja o "[Introdução ao monitoramento de desempenho do Active IQ Unified Manager](#)" para mais informações.

- Diagnosticando e gerenciando problemas de capacidade de volume

Se problemas de capacidade de armazenamento de volume forem exibidos na página Painel, os administradores de armazenamento podem seguir os links incorporados para visualizar as tendências atuais e históricas relacionadas à capacidade de armazenamento do volume afetado, visualizar conselhos sobre solução de problemas e atribuir a resolução de problemas a outros administradores.

- Configurando, monitorando e diagnosticando problemas de relacionamento de proteção

Depois de criar e configurar relacionamentos de proteção, os administradores de armazenamento podem visualizar os possíveis problemas relacionados aos relacionamentos de proteção, o estado atual dos relacionamentos de proteção, as informações atuais e históricas sobre o sucesso das tarefas de proteção sobre os relacionamentos afetados e conselhos para solução de problemas. Veja o "[Criação, monitoramento e solução de problemas de relacionamentos de proteção](#)" para mais informações.

- Criação de arquivos de backup e restauração de dados de arquivos de backup.
- Associando objetos de armazenamento com anotações

Ao associar objetos de armazenamento a anotações, os administradores de armazenamento podem filtrar e visualizar os eventos relacionados aos objetos de armazenamento, o que permite que os administradores de armazenamento priorizem e resolvam os problemas associados aos eventos.

- Use APIs REST para ajudar a gerenciar seus clusters visualizando as informações de integridade, capacidade e desempenho capturadas pelo Unified Manager. Ver "[Introdução às APIs REST do Active IQ Unified Manager](#)" para mais informações.
- Enviando 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. Pacotes de suporte devem ser enviados ao suporte técnico quando o problema exigir diagnóstico e solução de problemas mais detalhados do que os fornecidos por uma mensagem do AutoSupport .

Monitorar e solucionar problemas de disponibilidade de dados

O Unified Manager monitora a confiabilidade com que usuários autorizados podem

acessar seus dados armazenados, alerta você sobre condições que bloqueiam ou impedem esse acesso e permite que você diagnostique essas condições e atribua e acompanhe sua resolução.

Os tópicos do fluxo de trabalho de disponibilidade nesta seção descrevem exemplos de como um administrador de armazenamento pode usar a interface de usuário da Web do Unified Manager para descobrir, diagnosticar e atribuir para resolução condições de hardware e software que afetam negativamente a disponibilidade de dados.

Verificar e resolver condições de inatividade do link de interconexão de failover de armazenamento

Este fluxo de trabalho fornece um exemplo de como você pode verificar, avaliar e resolver condições de link de interconexão de failover de armazenamento inativo. Neste cenário, você é um administrador que usa o Unified Manager para verificar riscos de failover de armazenamento antes de iniciar uma atualização de versão do ONTAP em seus nós.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Se as interconexões de failover de armazenamento entre nós de pares 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 armazenamento nos nós do cluster alvos da 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 **Nome** da página de inventário **Gerenciamento de eventos**, clique em  e entrar *failover na caixa de texto para limitar o evento a ser exibido para eventos relacionados a failover de armazenamento.

Todos os eventos anteriores relacionados às condições de failover de armazenamento são exibidos.

Neste cenário, o Unified Manager exibe o evento “Storage Failover Interconnect One or More Links Down” na seção 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 detalhes do evento.

Neste exemplo, você clica no título do evento “Storage Failover Interconnect One or More Links Down”.

A página Detalhes do evento é exibida.

- a. Na página Detalhes do evento, você pode executar uma ou mais das seguintes tarefas:
 - Revise a mensagem de erro no campo Causa e avalie o problema.
 - Atribua o evento a um administrador.

- Reconheça o evento.

Informações relacionadas

["Página de detalhes do evento"](#)

["Funções e recursos do usuário do Unified Manager"](#)

Executar ação corretiva para links de interconexão de failover de armazenamento inativos

Ao exibir a página Detalhes do evento de um evento relacionado a 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

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Neste cenário de exemplo, o resumo do evento fornecido na página 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 do evento de exemplo indicam que um link de interconexão de failover de armazenamento, Link1, entre os nós do par HA aardvark e bonobo está inativo, mas que o Link0 entre Apple e Boy está ativo. Como um link está ativo, o acesso remoto à memória dinâmica (RDMA) ainda está funcionando e uma tarefa de failover de armazenamento ainda pode ser bem-sucedida.

No entanto, para garantir que ambos os links não falhem e que a proteção contra failover de armazenamento seja totalmente desabilitada, você decide diagnosticar melhor o motivo da queda do Link1.

Passos

1. Na página de detalhes do **Evento**, você pode clicar no link para o evento especificado no campo Origem para obter mais detalhes de outros eventos que podem estar relacionados à condição de link de interconexão de failover de armazenamento inativo.

Neste exemplo, a origem do evento é o nó chamado aardvark. Clicar no nome desse nó exibe os Detalhes de HA para o par de HA afetado, aardvark e bonobo, na guia Nós da página Detalhes do cluster/saúde, e exibe outros eventos que ocorreram recentemente no par de HA afetado.

2. Confira os **Detalhes do HA** para mais informações relacionadas ao evento.

Neste exemplo, as informações relevantes estão na tabela Eventos. A tabela mostra o evento “Storage Failover Connection One or More Link Down”, o horário em que o evento foi gerado e, novamente, o nó de onde esse evento se originou.

Usando as informações de localização do nó nos Detalhes do HA, solicite ou conclua pessoalmente uma inspeção física e reparo do problema de failover de armazenamento nos nós do par HA afetados.

Informações relacionadas

["Página de detalhes do evento"](#)

["Funções e recursos do usuário do Unified Manager"](#)

Resolver problemas de volume offline

Este fluxo de trabalho fornece um exemplo de como você pode avaliar e resolver um evento offline de volume que o Unified Manager pode exibir na página de inventário do Gerenciamento de Eventos. Neste cenário, você é um administrador que usa o Unified Manager para solucionar problemas de um ou mais eventos de volume offline.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Os volumes podem ser relatados offline por vários motivos:

- O administrador do SVM deliberadamente colocou o volume offline.
- O nó do cluster de hospedagem do volume está inativo e o failover de armazenamento para seu parceiro de par de HA também falhou.
- A máquina virtual de armazenamento (SVM) de hospedagem do volume foi interrompida porque o nó que hospeda o volume raiz dessa SVM está inativo.
- O agregado de hospedagem do volume está inativo devido à falha simultânea de dois discos RAID.

Você pode usar a página de inventário do Gerenciamento de Eventos e as páginas de detalhes do Cluster/Integridade, VM de Armazenamento/Integridade e Volume/Integridade 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 Detalhes do evento para o incidente de disponibilidade é exibida.

4. Nessa página, verifique as notas para ver se há alguma indicação de que o administrador do 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:

- Revise as informações exibidas no campo Causa para possível orientação de diagnóstico.

Neste exemplo, as informações no campo Causa informam apenas que o volume está offline.

- Verifique a área Notas e Atualizações para ver se há alguma indicação de que o administrador do SVM colocou deliberadamente o volume em questão offline.
- Clique na origem do evento, neste caso o volume relatado offline, para obter mais informações sobre esse volume.
- Atribua o evento a um administrador.
- Reconheça o evento ou, se apropriado, marque-o como resolvido.

Executar ações de diagnóstico para condições de volume offline

Depois de navegar até a página de detalhes de Volume/Saúde de um volume relatado como offline, você pode pesquisar informações adicionais úteis para diagnosticar a condição de volume offline.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Se o volume relatado como offline não foi colocado offline deliberadamente, ele pode estar offline por vários motivos.

A partir da página de detalhes Volume/Saúde do volume offline, você 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 offline porque seu nó host está inativo e o failover de armazenamento para seu parceiro de par HA também falhou.

Ver "[Determinando se uma condição de volume offline é causada por um nó inativo](#)".

- Clique nos links da página de detalhes de **Volume / Saúde** para determinar se o volume está offline e se sua máquina virtual de armazenamento host (SVM) está parada porque o nó que hospeda o volume raiz dessa SVM está inativo.

Ver "[Determinar se um volume está offline e o SVM foi interrompido porque um nó está inativo](#)".

- Clique nos links da página de detalhes **Volume / Saúde** para determinar se o volume está offline devido a discos quebrados em seu agregado de host.

Ver "[Determinar se um volume está offline devido a discos quebrados em um agregado](#)".

Informações relacionadas

["Funções e recursos do usuário do Unified Manager"](#)

Determinar se um volume está offline porque seu nó host está inativo

Você pode usar a interface de usuário da Web do Unified Manager para confirmar ou

eliminar a possibilidade de um volume estar offline porque seu nó host está inativo e que o failover de armazenamento para seu parceiro de par de HA não foi bem-sucedido.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Para determinar se a condição de volume offline é causada por falha do nó de hospedagem e subsequente failover de armazenamento malsucedido, execute as seguintes ações:

Passos

1. Localize e clique no link de hipertexto exibido em SVM no painel **Dispositivos relacionados** da página de detalhes **Volume / Saúde** do volume offline.

A página Detalhes da VM de armazenamento/Integridade exibe informações sobre a máquina virtual de armazenamento (SVM) que hospeda o volume offline.

2. No painel **Dispositivos relacionados** da página de detalhes **VM de armazenamento / Integridade**, localize e clique no link de hipertexto exibido em Volumes.

A exibição Saúde: Todos os volumes exibe uma tabela de informações sobre todos os volumes hospedados pelo SVM.

3. No cabeçalho da coluna Estado da visualização **Saúde: Todos os volumes**, clique no símbolo de filtro  e, em seguida, selecione a opção **Offline**.

Somente os volumes SVM que estão em estado offline são listados.

4. Na visualização Saúde: Todos os volumes, clique no símbolo de grade  e, em seguida, selecione a opção **Nós de cluster**.

Pode ser necessário rolar na caixa de seleção da grade para localizar a opção **Nós do Cluster**.

A coluna Nós do Cluster é adicionada ao inventário de volumes e exibe o nome do nó que hospeda cada volume offline.

5. Na exibição **Saúde: Todos os volumes**, localize a listagem do volume offline e, na coluna Nó do cluster, clique no nome do 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 na exibição.

Após confirmar que a condição de volume offline existe porque o nó do host está inativo e o failover de armazenamento para o parceiro do par HA falhou, entre em contato com o administrador ou operador apropriado para reiniciar manualmente o nó inativo e corrigir o problema de failover de armazenamento.

Determinar se um volume está offline e seu SVM está parado porque um nó está inativo

Você pode usar a interface de usuário da Web do Unified Manager para confirmar ou eliminar a possibilidade de um volume estar offline porque sua máquina virtual de armazenamento host (SVM) está parada porque o nó que hospeda o volume raiz dessa SVM está inativo.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Para determinar se a condição de volume offline é causada pela parada do SVM host porque o nó que hospeda o volume raiz desse SVM está inativo, execute as seguintes ações:

Passos

1. Localize e clique no link de hipertexto exibido sob o SVM no painel **Dispositivos relacionados** da página de detalhes **Volume / Saúde** do volume offline.

A página de detalhes da VM de armazenamento/integridade exibe o status “em execução” ou “parado” da SVM de hospedagem. Se o status do SVM for em execução, a condição de volume offline não será causada pelo nó que hospeda o volume raiz desse SVM estar inativo.

2. Se o status do SVM for interrompido, clique em **Exibir SVMs** para identificar melhor a causa da interrupção do SVM de hospedagem.
3. No cabeçalho da coluna SVM da visualização **Saúde: Todas as VMs de armazenamento**, clique no símbolo de filtro  e então digite o nome do SVM parado.

As informações para esse SVM são mostradas em uma tabela.

4. Na visualização **Saúde: Todas as VMs de armazenamento**, clique em  e então selecione a opção **Volume Raiz**.

A coluna Volume raiz é adicionada ao inventário do SVM e exibe o nome do volume raiz do SVM interrompido.

5. Na coluna Volume raiz, clique no nome do volume raiz para exibir a página de detalhes **VM de armazenamento / Integridade** desse volume.

Se o status do volume raiz do SVM for (Online), a condição offline do volume 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 do SVM.
7. Localize e clique no link de hipertexto exibido em Nó no painel **Dispositivos relacionados** da página de detalhes **Agregado / Saúde** do Agregado.

A guia Nós na página Detalhes do cluster/integridade exibe o estado do par de nós de HA ao qual o nó de hospedagem do volume raiz SVM pertence. O estado do nó é indicado no visor.

Após confirmar que a condição de volume offline é causada pela condição de SVM do host desse volume offline, que por sua vez é causada pelo nó que hospeda o volume raiz desse SVM estar inativo, entre em contato com o administrador ou operador apropriado para reiniciar manualmente o nó inativo.

Determinar se um volume está offline devido a discos quebrados em um agregado

Você pode usar a interface da Web do Unified Manager para confirmar ou eliminar a possibilidade de um volume estar offline porque problemas no disco RAID deixaram seu agregado de host offline.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Para determinar se a condição do volume offline é causada por problemas no disco RAID que estão deixando o agregado de hospedagem offline, execute as seguintes ações:

Passos

1. Localize e clique no link de hipertexto exibido em Agregado no painel **Dispositivos relacionados** da página de detalhes **Volume / Saúde**.

A página Detalhes do agregado/saúde exibe o status online ou offline do agregado de hospedagem. Se o status agregado for online, os problemas no disco RAID não serão a causa do volume estar offline.

2. Se o status agregado for offline, clique em **Informações do disco** e procure por eventos de disco quebrado na lista **Eventos** na guia **Informações do disco**.
3. Para identificar melhor os discos quebrados, clique no link de hipertexto exibido em Nó no painel **Dispositivos relacionados**.

A página Detalhes do Cluster/Saúde é exibida.

4. Clique em **Discos** e selecione **Quebrado** no painel **Filtros** para listar todos os discos em estado quebrado.

Se os discos no estado quebrado causaram o estado offline do agregado do host, o nome do agregado será exibido na coluna Agregado impactado.

Após confirmar que a condição de volume offline é causada por discos RAID quebrados e o consequente agregado de host offline, entre em contato com o administrador ou operador apropriado para substituir manualmente os discos quebrados e colocar o agregado online novamente.

Resolver problemas de capacidade

Este fluxo de trabalho fornece um exemplo de como você pode resolver um problema de capacidade. Neste cenário, você é um administrador ou operador e acessa a página Unified ManagerDashboard para verificar se algum dos objetos de armazenamento monitorados tem problemas de capacidade. Você quer determinar a possível causa e solução do problema.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Na página Painel, procure por um evento de erro “Volume Space Full” no painel Capacidade, na lista suspensão de eventos.

Passos

1. No painel **Capacidade** da página **Painel**, clique no nome do evento de erro Espaço de Volume Cheio.

A página Detalhes do evento para o erro 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 e clique nas sugestões em Ações corretivas sugeridas para revisar as descrições de possíveis correções.
 - Clique no nome do objeto, neste caso um volume, no campo Origem para obter detalhes sobre o objeto.

- Procure por notas que possam ter sido adicionadas sobre este evento.
- Adicione uma nota ao evento.
- Atribuir o evento a outro usuário.
- Reconheça o evento.
- Marque o evento como resolvido.

Informações relacionadas

["Página de detalhes do evento"](#)

Execute as ações corretivas sugeridas para um volume total

Após receber um evento de erro “Volume Space Full”, você revisa as ações corretivas sugeridas na página Detalhes do evento e decide executar uma das ações sugeridas.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Um usuário com qualquer função pode executar todas as tarefas neste fluxo de trabalho que usam o Unified Manager.

Neste exemplo, você viu um evento de erro de Espaço de Volume Cheio na página de inventário do Unified Manager Event Management e clicou no nome do evento.

Possíveis ações corretivas que você pode executar para um volume completo incluem o seguinte:

- Habilitando crescimento automático, deduplicação ou compactação no volume
- Redimensionar ou mover o volume
- Excluir ou mover dados do volume

Embora todas essas ações devam ser executadas no ONTAP System Manager ou no ONTAP CLI, você pode usar o Unified Manager para encontrar informações que podem ser necessárias para determinar quais ações tomar.

Passos

1. Na página de detalhes do **Evento**, clique no nome do volume no campo Origem para visualizar detalhes sobre o volume afetado.
2. Na página de detalhes **Volume / Saúde**, clique em **Configuração** e veja que a deduplicação e a compactação já estão habilitadas no volume.

Você decide redimensionar o volume.

3. No painel **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 completo tem capacidade não comprometida suficiente, então você usa o ONTAP System Manager para redimensionar o volume, dando a ele mais capacidade.

Informações relacionadas

["Página de detalhes do evento"](#)

Gerenciar limites de saúde

Você pode configurar valores de limite de integridade global para todos os agregados, volumes e qtrees para rastrear quaisquer violações de limite de integridade.

Quais são os limites de integridade da capacidade de armazenamento

Um limite de integridade da capacidade de armazenamento é o ponto em que o servidor do Unified Manager gera eventos para relatar qualquer problema de capacidade com objetos de armazenamento. Você pode configurar alertas para enviar notificações sempre que tais eventos ocorrerem.

Os limites de integridade da capacidade de armazenamento 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 as definições globais de limite de saúde

Você pode configurar condições globais de limite de integridade para capacidade, crescimento, reserva de Snapshot, cotas e inodes para monitorar seu agregado, volume e tamanho de qtree de forma eficaz. Você também pode editar as configurações para gerar eventos para exceder limites de atraso.

As configurações de limite de integridade global se aplicam a todos os objetos aos quais estão associadas, como agregados, volumes e assim por diante. Quando os limites são ultrapassados, um evento é gerado e, se alertas estiverem 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 tornam-se obsoletos no próximo ciclo de monitoramento.

As configurações de limite de integridade global podem ser acessadas na seção Limites de eventos do menu de navegação à esquerda. Você também pode modificar as configurações de limite para objetos individuais, na página de inventário ou na página de detalhes desse objeto.

- Para obter informações, consulte ["Configurando valores de limite de integridade agregada global"](#).

Você pode configurar as configurações de limite de integridade para capacidade, crescimento e cópias de instantâneo para todos os agregados para rastrear qualquer violação de limite.

- Para obter informações, consulte ["Configurando valores de limite de integridade de volume global"](#).

Você pode editar as configurações de limite de integridade para capacidade, cópias de instantâneo, cotas de qtree, crescimento de volume, substituição de espaço de reserva e inodes para todos os volumes para rastrear qualquer violação de limite.

- Para obter informações, consulte ["Configurando valores de limite de integridade do qtree global"](#).

Você pode editar as configurações de limite de integridade para capacidade de todas as qtrees para rastrear qualquer violação de limite.

- Para obter informações, consulte ["Editando configurações de limite de integridade de atraso para relacionamentos de proteção não gerenciados"](#).

Você pode aumentar ou diminuir a porcentagem de tempo de atraso do aviso ou erro para que os eventos sejam gerados em intervalos mais apropriados às suas necessidades.

Configurar valores de limite de integridade agregada global

Você pode configurar valores de limite de integridade global 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

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Quando você configura as opções globalmente, os valores padrão dos objetos são modificados. Entretanto, se os valores padrão forem 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 para atender aos requisitos do seu ambiente.

Quando o crescimento automático é habilitado em volumes que residem no agregado, os limites de capacidade do agregado são considerados violados com base no tamanho máximo do volume definido pelo crescimento automático, não com base no tamanho do volume original.



Os valores limite de integridade não são aplicáveis ao agregado raiz do nó.

Passos

1. No painel de navegação esquerdo, clique em **Limites de evento > Agregar**.
2. Configure os valores de limite apropriados para capacidade, crescimento e cópias de instantâneo.
3. Clique em **Salvar**.

Informações relacionadas

["Adicionando usuários"](#)

Configurar valores de 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 saúde, 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

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

A maioria das opções de limite tem valores padrão para melhor monitoramento. No entanto, você pode alterar os valores para adequá-los aos requisitos do seu ambiente.

Observe que quando o crescimento automático é habilitado 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 de 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 do Snapshot atingir 250. Se desejar definir esse limite para menos de 250 para essas versões mais antigas, você deve defini-lo para 250 ou menos aqui, na visualização Saúde: Todos os volumes ou na página de detalhes do Volume/Saúde.

Passos

1. No painel de navegação esquerdo, clique em **Limites de evento > Volume**.
2. Configure os valores de limite apropriados para capacidade, cópias de instantâneo, cotas de qtree, crescimento de volume e inodes.
3. Clique em **Salvar**.

Informações relacionadas

["Adicionando usuários"](#)

Configurar valores de limite de integridade do qtree global

Você pode configurar os valores de limite de integridade global para todas as qtrees para rastrear qualquer violação de limite. Eventos apropriados são gerados para violações de limites de saúde, 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 todas as qtrees monitoradas.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

As opções de limite têm valores padrão para melhor monitoramento; no entanto, você pode alterar os valores para atender aos requisitos do seu ambiente.

Os eventos são gerados para uma qtree somente quando uma cota de Qtree ou uma cota padrão é definida na qtree. Os eventos não serão gerados se o espaço definido em uma cota de usuário ou cota de grupo exceder o limite.

Passos

1. No painel de navegação esquerdo, clique em **Limites de evento > Qtree**.
2. Configure os valores de limite de capacidade apropriados.
3. Clique em **Salvar**.

Configurar configurações de limite de atraso para relacionamentos de proteção não gerenciados

Você pode editar as configurações globais de limite de integridade de erro e aviso de atraso padrão para relacionamentos de proteção não gerenciados, para que os eventos

sejam gerados em intervalos apropriados às suas necessidades.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

O tempo de atraso não deve ser maior que o intervalo definido no cronograma de transferência. Por exemplo, se o cronograma 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 maior que 1,5 hora.

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 um relacionamento de proteção não gerenciado.

Passos

1. No painel de navegação esquerdo, clique em **Limites de evento > Relacionamento**.
2. Aumente ou diminua a porcentagem global de tempo de atraso de aviso ou erro padrão, conforme necessário.
3. Para desabilitar o acionamento de um evento de aviso ou erro a partir de qualquer limite de atraso, desmarque a caixa ao lado de **Ativado**.
4. Clique em **Salvar**.

Informações relacionadas

["Adicionando usuários"](#)

Editar configurações individuais de limite de integridade agregada

Você pode editar as configurações de limite de integridade para capacidade agregada, crescimento e cópias de instantâneo de um ou mais agregados. Quando um limite é ultrapassado, alertas são gerados e você recebe notificações. Essas notificações ajudam você a tomar medidas preventivas com base no evento gerado.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Com base nas alterações nos valores limite, os eventos são gerados ou tornados obsoletos no próximo ciclo de monitoramento.

Quando o crescimento automático é habilitado em volumes que residem no agregado, os limites de capacidade do agregado 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 esquerdo, clique em **Armazenamento > Agregados**.
2. Na exibição **Saúde: Todos os agregados**, selecione um ou mais agregados e clique em **Editar limites**.
3. Na caixa de diálogo **Editar Limites de Agregação**, edite as configurações de limite de um dos seguintes: capacidade, crescimento ou cópias de instantâneo, marcando a caixa de seleção apropriada e modificando as configurações.

4. Clique em **Salvar**.

Informações relacionadas

["Adicionando usuários"](#)

Editar configurações 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 ultrapassado, alertas são gerados e você recebe notificações. Essas notificações ajudam você a tomar medidas preventivas com base no evento gerado.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Com base nas alterações nos valores limite, os eventos são gerados ou tornados obsoletos no próximo ciclo de monitoramento.

Observe que quando o crescimento automático é habilitado 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 de 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 do Snapshot atingir 250. Se desejar definir esse limite para menos de 250 para essas versões mais antigas, você deve defini-lo para 250 ou menos aqui, na visualização Saúde: Todos os volumes ou na página de detalhes do Volume/Saúde.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > 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 um dos seguintes: capacidade, cópias de instantâneo, cota qtree, crescimento ou inodes, marcando a caixa de seleção apropriada e modificando as configurações.
4. Clique em **Salvar**.

Informações relacionadas

["Adicionando usuários"](#)

Editar configurações individuais de limite de integridade do qtree

Você pode editar as configurações de limite de integridade para capacidade de qtree para uma ou mais qtrees. Quando um limite é ultrapassado, alertas são gerados e você recebe notificações. Essas notificações ajudam você a tomar medidas preventivas com base no evento gerado.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Com base nas alterações nos valores limite, os eventos são gerados ou tornados obsoletos no próximo ciclo de monitoramento.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Qtrees**.
2. Na visualização **Capacidade: Todas as Qtrees**, selecione uma ou mais qtrees e clique em **Editar Limites**.
3. Na caixa de diálogo **Editar Limites de Qtree**, altere os limites de capacidade para a qtree ou qtrees selecionadas e clique em **Salvar**.



Você também pode definir limites individuais de qtree na guia Qtrees na página de detalhes da VM de armazenamento/integridade.

Gerenciar objetivos de segurança do cluster

O Unified Manager fornece um painel que identifica o quão seguros são seus clusters ONTAP , máquinas virtuais de armazenamento (SVMs) e volumes com base nas recomendações definidas no *Guia de reforço de segurança da NetApp para ONTAP 9*.

O objetivo do painel de segurança é mostrar todas as áreas em que seus clusters ONTAP não estão alinhados com as diretrizes recomendadas da NetApp para que você possa corrigir esses possíveis problemas. Na maioria dos casos, você corrigirá os problemas usando o ONTAP System Manager ou o ONTAP CLI. Sua organização pode não seguir todas as recomendações, então, em alguns casos, você não precisará fazer nenhuma alteração.

Veja o "[Guia de reforço de segurança da NetApp para ONTAP 9](#)" (TR-4569) para recomendações e resoluções detalhadas.

Além de relatar 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 seu administrador de armazenamento seja notificado quando novos eventos de segurança ocorrerem.

Para mais informações, consulte "[Quais critérios de segurança estão sendo avaliados](#)".

Quais critérios de segurança estão sendo avaliados

Em geral, os critérios de segurança para seus clusters ONTAP , máquinas virtuais de armazenamento (SVMs) e volumes estão sendo avaliados em relação às recomendações definidas no *Guia de reforço de segurança da 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 pareados têm sua comunicação criptografada
- se uma VM de armazenamento tem seu log de auditoria habilitado

- se seus volumes têm criptografia de software ou hardware habilitada

Veja os tópicos sobre categorias de conformidade e ["Guia de reforço de segurança da NetApp para ONTAP 9"](#) para obter informações detalhadas.



Eventos de atualização relatados pela plataforma Active IQ também são considerados eventos de segurança. Esses eventos identificam problemas cuja 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 mais informações, consulte ["Gerenciando objetivos de segurança do cluster"](#).

Categorias de conformidade do cluster

Esta tabela descreve os parâmetros de conformidade de segurança do cluster que o Unified Manager avalia, a recomendação da NetApp e se o parâmetro afeta a determinação geral de que o cluster está em conformidade ou não.

Ter SVMs não compatíveis em um cluster afetará o valor de conformidade do cluster. Portanto, em alguns casos, pode ser necessário corrigir problemas de segurança com uma SVM antes que a segurança do seu cluster seja considerada compatível.

Observe que nem todos os parâmetros listados abaixo aparecem para todas as instalações. Por exemplo, se você não tiver clusters pareados ou se tiver desabilitado o AutoSupport em um cluster, você não verá os itens Peering de Cluster ou AutoSupport de Transporte HTTPS na página da interface do usuário.

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
FIPS globais	Indica se o modo de conformidade Global FIPS (Federal Information Processing Standard) 140-2 está habilitado ou desabilitado. Quando o FIPS está ativado, TLSv1 e SSLv3 são desativados, e somente TLSv1.1 e TLSv1.2 são permitidos.	Habilitado	Sim
Telnet	Indica se o acesso Telnet ao sistema está habilitado ou desabilitado. A NetApp recomenda o Secure Shell (SSH) para acesso remoto seguro.	Desabilitado	Sim
Configurações SSH inseguras	Indica se o SSH usa cifras inseguras, por exemplo, cifras que começam com *cbc.	Não	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
Banner de login	Indica se o banner de login está habilitado ou desabilitado para usuários que acessam o sistema.	Habilitado	Sim
Cluster Peering	Indica se a comunicação entre clusters pareados é criptografada ou não criptografada. A criptografia deve ser configurada nos clusters de origem e de destino para que este parâmetro seja considerado compatível.	Criptografado	Sim
Protocolo de Tempo 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	A partir da versão 9.14.1, o Active IQ Unified Manager fornece informações de status do Protocolo de Status de Certificado Online (OCSP) no nível da máquina virtual de armazenamento (SVM, anteriormente conhecida como Vserver). Isso significa que a validação OCSP é aplicada a todas as conexões SSL/TLS feitas ao SVM e garante a integridade e a validade dos certificados usados nessas conexões.	Habilitado	Não
Registro de auditoria remota	Indica se o encaminhamento de log (Syslog) é criptografado ou não.	Criptografado	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
Transporte HTTPS de AutoSupport	Indica se HTTPS é usado como o protocolo de transporte padrão para enviar mensagens do AutoSupport ao suporte da NetApp .	Habilitado	Sim
Usuário administrador padrão	Indica se o Usuário Administrador Padrão (integrado) está habilitado ou desabilitado. A NetApp recomenda bloquear (desabilitar) quaisquer contas internas desnecessárias.	Desabilitado	Sim
Usuários SAML	Indica se o SAML está configurado. O SAML permite que você configure a autenticação multifator (MFA) como um método de login para logon único.	Não	Não
Usuários do Active Directory	Indica se o Active Directory está configurado. O Active Directory e o LDAP são os mecanismos de autenticação preferenciais para usuários que acessam clusters.	Não	Não
Usuários LDAP	Indica se o LDAP está configurado. O Active Directory e o LDAP são os mecanismos de autenticação preferenciais para usuários que gerenciam clusters por meio de usuários locais.	Não	Não
Usuários de Certificados	Indica se um usuário de certificado está configurado para efetuar login no cluster.	Não	Não

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
Usuários locais	Indica se os usuários locais estão configurados para efetuar login no cluster.	Não	Não
Shell Remoto	Indica se o RSH está habilitado. Por razões de segurança, o RSH deve ser desabilitado. O Secure Shell (SSH) para acesso remoto seguro é o preferido.	Desabilitado	Sim
MD5 em uso	Indica se as contas de usuário do ONTAP usam a função MD5 Hash menos segura. A migração de contas de usuários com hash MD5 para a função de 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 armazenamento

Esta tabela descreve os critérios de conformidade de segurança da máquina virtual de armazenamento (SVM) que o Unified Manager avalia, a recomendação da NetApp e se o parâmetro afeta a determinação geral de que a SVM está em conformidade ou não.

Parâmetro	Descrição	Recomendação	Afeta a conformidade do SVM
Registro de auditoria	Indica se o registro de auditoria está habilitado ou desabilitado.	Habilitado	Sim
Configurações SSH inseguras	Indica se o SSH usa cifras inseguras, por exemplo, cifras que começam com cbc* .	Não	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do SVM
Banner de login	Indica se o banner de login está habilitado ou desabilitado para usuários que acessam SVMs no sistema.	Habilitado	Sim
Criptografia LDAP	Indica se a criptografia LDAP está habilitada ou desabilitada.	Habilitado	Não
Autenticação NTLM	Indica se a autenticação NTLM está habilitada ou desabilitada.	Habilitado	Não
Assinatura de carga útil LDAP	Indica se a assinatura de carga útil LDAP está habilitada ou desabilitada.	Habilitado	Não
Configurações do CHAP	Indica se o CHAP está habilitado ou desabilitado.	Habilitado	Não
Kerberos V5	Indica se a autenticação Kerberos V5 está habilitada ou desabilitada.	Habilitado	Não
Autenticação NIS	Indica se o uso da autenticação NIS está configurado.	Desabilitado	Não
Status do FPolicy ativo	Indica se FPolicy foi criado ou não.	Sim	Não
Criptografia SMB habilitada	Indica se a assinatura e selagem SMB não está habilitada.	Sim	Não
Assinatura SMB habilitada	Indica se a assinatura SMB não está habilitada.	Sim	Não

Categorias de conformidade de volume

Esta tabela descreve os parâmetros de criptografia de volume que o Unified Manager avalia para determinar se os dados em seus volumes estão adequadamente protegidos contra acesso por 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 soluções de criptografia de software NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
Hardware criptografado	Exibe o número de volumes protegidos usando a criptografia de hardware NetApp Storage Encryption (NSE).
Software e hardware criptografados	Exibe o número de volumes protegidos por criptografia de software e hardware.
Não criptografado	Exibe o número de volumes que não estão criptografados.

O que significa não compatível

Clusters e máquinas virtuais de armazenamento (SVMs) são considerados não compatíveis quando qualquer um dos critérios de segurança que estão sendo avaliados em relação às recomendações definidas no *Guia de reforço de segurança da NetApp para ONTAP 9* não são atendidos. 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 está configurado conforme recomendado.
-  - O parâmetro não está configurado conforme recomendado.
-  - Ou a funcionalidade não está habilitada no cluster, ou o parâmetro não está configurado conforme recomendado, mas esse parâmetro não contribui para a conformidade do objeto.

Observe que o status da criptografia do volume não contribui para que o cluster ou o SVM sejam considerados compatíveis.

Exibir status de segurança para clusters e VMs de armazenamento

O Active IQ Unified Manager permite que você visualize o status de segurança dos objetos de armazenamento em seu ambiente de diferentes pontos na interface. Você pode coletar e analisar informações e relatórios com base em parâmetros definidos e detectar comportamento suspeito ou alterações não autorizadas no sistema nos clusters monitorados e VMs de armazenamento.

Para recomendações de segurança, consulte o "[Guia de reforço de segurança da NetApp para ONTAP 9](#)".

Exibir status de segurança em nível de objeto na página Segurança

Como administrador do sistema, você pode usar a página **Segurança** para obter visibilidade da força de segurança dos seus clusters ONTAP e VMs de armazenamento nos níveis de data center e site. Os objetos suportados são cluster, VMs de armazenamento e volumes. Siga estes passos:

Passos

1. No painel de navegação esquerdo, clique em **Painel**.
2. Dependendo se você deseja visualizar o status de segurança de todos os clusters monitorados ou de 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**. A página Segurança é exibida.

Clicando nos gráficos de barras, contagens e [View Reports](#) links levam você para a página Volumes, Clusters ou VMs de armazenamento para que você visualize os detalhes correspondentes ou gere relatórios, conforme necessário.

A página Segurança exibe os seguintes painéis:

- **Conformidade do Cluster:** o status de segurança (número de clusters que estão em conformidade ou não) de todos os clusters em um data center
- **Conformidade de VM de armazenamento:** o status de segurança (número de VMs de armazenamento que estão em conformidade ou não) para todas as VMs de armazenamento em seu data center
- **Criptografia de Volume:** o status de criptografia do volume (número de volumes criptografados ou não criptografados) de todos os volumes em seu ambiente
- **Status do Volume Anti-ransomware:** o status de segurança (número de volumes com anti-ransomware ativado ou desativado) de todos os volumes em seu ambiente
- **Autenticação e certificados de cluster:** o número de clusters usando cada tipo de método de autenticação, como SAML, Active 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 que você visualize o status de conformidade de segurança no nível do cluster.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Clusters**.
2. Selecione **Exibir > Segurança > Todos os clusters**.

Parâmetros de segurança padrão, como FIPS global, Telnet, configurações SSH inseguras, banner de login, protocolo de tempo de rede, AutoSupport HTTPS Transport e o status de expiração do certificado do cluster são exibidos.

Você pode clicar no ⓘ botão mais opções e escolha visualizar os detalhes de segurança na página **Segurança** do Unified Manager ou no System Manager. Você deve ter credenciais válidas para visualizar os detalhes no Gerenciador do Sistema.



Se um cluster tiver um certificado expirado, você pode clicar em `expired` em **Validade do Certificado de Cluster** e renove-o no Gerenciador do Sistema (9.10.1 e posterior). Você não pode clicar `expired` se a instância do System Manager for de uma versão anterior à 9.10.1.

Visualize detalhes de segurança de todos os clusters na página de VMs de armazenamento

A página de detalhes **VMs de armazenamento / Segurança** permite que você visualize o status de conformidade de segurança no nível da VM de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > VMs de armazenamento**.
2. Selecione **Exibir > Segurança > Todas as VMs de armazenamento**. Uma lista de clusters com os parâmetros de segurança é exibida.

Você pode ter uma visão 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 escolha visualizar os detalhes de segurança na página **Segurança** do Unified Manager ou no System Manager. Você deve ter credenciais válidas para visualizar os detalhes no Gerenciador do Sistema.

Para obter detalhes de segurança anti-ransomware para volumes e VMs de armazenamento, consulte "[Visualizando o status anti-ransomware de todos os volumes e VMs de armazenamento](#)".

Visualize eventos de segurança que podem exigir atualizações de software ou firmware

Há certos eventos de segurança que têm uma área de impacto de “Atualização”. Esses eventos são relatados pela plataforma Active IQ e identificam problemas cuja 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

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Talvez você queira executar ações corretivas imediatas para alguns desses problemas, enquanto outros 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 determinados eventos de atualização de segurança sobre os quais você não deseja ser notificado, esta lista pode ajudar a identificá-los 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.

Veja como a autenticação do usuário está sendo gerenciada em todos os clusters

A página Segurança exibe os tipos de autenticação usados para autenticar usuários em cada cluster e o número de usuários que estão acessando o cluster usando cada tipo. Isso permite que você verifique se a autenticação do usuário está sendo realizada com

segurança, conforme definido pela sua organização.

Passos

1. No painel de navegação esquerdo, clique em **Painel**.
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. Visualize o cartão **Autenticação de Cluster** para ver o número de usuários que estão acessando o sistema usando cada tipo de autenticação.
5. Visualize o cartão **Segurança do Cluster** para visualizar os mecanismos de autenticação usados para autenticar usuários em cada cluster.

Se houver alguns usuários acessando o sistema usando um método inseguro ou usando um método não recomendado pela NetApp, você poderá desabilitar o método.

Visualizar o status de criptografia de todos os volumes

Você pode visualizar uma lista de todos os volumes e seus status de criptografia atuais para poder determinar se os dados em seus volumes estão adequadamente protegidos contra acesso por usuários não autorizados.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Os tipos de criptografia que podem ser aplicados a um volume são:

- Software - Volumes protegidos usando soluções de criptografia de software NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
- Hardware - Volumes protegidos usando criptografia de hardware NetApp Storage Encryption (NSE).
- Software e Hardware - Volumes protegidos por criptografia de software e hardware.
- Nenhum - Volumes que não são criptografados.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Saúde > Criptografia de Volumes**.
3. Na exibição **Saúde: Criptografia de volumes**, classifique pelo campo **Tipo de criptografia** ou use o Filtro para exibir volumes que têm um tipo de criptografia específico ou que não são criptografados (Tipo de criptografia "Nenhum").

Visualizando o status anti-ransomware de todos os volumes e VMs de armazenamento

Você pode visualizar uma lista de todos os volumes e VMs de armazenamento (SVMs) e seus status anti-ransomware atuais para que possa determinar se os dados em seus volumes e SVMs estão adequadamente protegidos contra ataques de ransomware.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Para obter mais informações sobre os diferentes status anti-ransomware, consulte ["ONTAP: Habilitar anti-](#)

Visualize detalhes de segurança de todos os volumes com detecção anti-ransomware

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Saúde > Segurança > Anti-ransomware**
3. Na exibição **Segurança: Anti-ransomware**, você pode classificar pelos vários campos ou usar o Filtro.



O anti-ransomware não é compatível com volumes offline, volumes restritos, volumes SnapLock , volumes FlexGroup , volumes FlexCache , volumes somente SAN, volumes de VMs de armazenamento interrompidas, volumes raiz de VMs de armazenamento ou volumes de proteção de dados.

Visualize detalhes de segurança de todas as VMs de armazenamento com detecção anti-ransomware

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > VMs de armazenamento**.
2. Selecione **Exibir > Segurança > Anti-ransomware**. Uma lista de SVMs com status anti-ransomware é exibida.



O monitoramento anti-ransomware não é suportado em VMs de armazenamento que não tenham o protocolo NAS habilitado.

Ver todos os eventos de segurança ativos

Você pode visualizar todos os eventos de segurança ativos e atribuir cada um deles a um usuário que pode resolver o problema. Além disso, se houver determinados eventos de segurança que você não deseja receber, esta lista pode ajudá-lo a identificar os eventos que você deseja desabilitar.

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos 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, assim como quaisquer outros eventos recebidos pelo Unified Manager. Além disso, se você quiser

tratar todos os eventos de segurança da mesma forma e enviar e-mails para a mesma pessoa, poderá criar um único alerta para notificá-lo quando algum evento de segurança for acionado.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

O exemplo abaixo mostra como criar um alerta para o evento de segurança “Protocolo Telnet habilitado”. 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 você deseja habilitar este 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 habilitado**.
6. Clique em **Ações** e selecione o nome do usuário que receberá o e-mail de alerta no campo **Alertar estes 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**.

Desabilitar eventos de segurança específicos

Todos os eventos são ativados por padrão. Você pode desabilitar eventos específicos para impedir a geração de notificações para aqueles eventos que não são importantes no seu ambiente. Você pode habilitar eventos que estão desabilitados se quiser voltar a receber notificações sobre eles.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Quando você desabilita eventos, os eventos gerados anteriormente no sistema são marcados como obsoletos, e os alertas configurados para esses eventos não são acionados. Quando você habilita eventos que estão desabilitados, as notificações para esses eventos são geradas a partir do próximo ciclo de monitoramento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Configuração de evento**.
2. Na página Configuração de **Evento**, desabilite ou habilite eventos escolhendo uma das seguintes opções:

Se você quiser...	Então faça isto...
Desativar eventos	a. Clique em Desativar. b. Na caixa de diálogo Desativar eventos, selecione a gravidade Aviso. Esta é a categoria para todos os eventos de segurança. c. Na coluna Eventos correspondentes, selecione os eventos de segurança que você deseja desabilitar e clique na seta para a direita para mover esses eventos para a coluna Desabilitar eventos. d. Clique em Salvar e Fechar. e. Verifique se os eventos que você desativou são exibidos na exibição de lista da página Configuração de eventos.
Habilitar eventos	a. Na lista de eventos desabilitados, marque a caixa de seleção do evento ou eventos que você deseja reativar. b. Clique em Ativar.

Eventos de segurança

Os eventos de segurança fornecem informações sobre o status de segurança de clusters ONTAP , máquinas virtuais de armazenamento (SVMs) e volumes com base em parâmetros definidos no *Guia de reforço de segurança da NetApp para ONTAP 9*. Esses eventos notificam você sobre possíveis problemas para que você possa avaliar a gravidade e corrigi-los, se necessário.

Os eventos de segurança são agrupados por tipo de origem e incluem o nome do evento e da armadilha, o nível de impacto e a gravidade. Esses eventos aparecem nas categorias de eventos de cluster e VM de armazenamento.

Gerenciar operações de backup e restauração

Você pode criar backups do Active IQ Unified Manager e usar o recurso de restauração para restaurar o backup no mesmo sistema (local) ou em 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 que estão sendo gerenciados:

Sistema operacional	Tamanho da implantação	Método de backup recomendado
VMware vSphere	Qualquer	Instantâneo do VMware do appliance virtual do 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	Instantâneo do NetApp do banco de dados do Unified Manager
Microsoft Windows	Pequeno	Despejo de banco de dados MySQL do Unified Manager
	Grande	Instantâneo do NetApp 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 no appliance 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 seguintes tarefas permitem que você conclua um backup do dispositivo virtual:

1. Desligue a VM e faça um snapshot do appliance virtual do Unified Manager.
2. Faça uma cópia do NetApp Snapshot no armazenamento de dados para capturar o snapshot do VMware.

Se o armazenamento de dados não estiver hospedado em um sistema executando o software ONTAP , siga as diretrizes do fornecedor de armazenamento para criar um backup do snapshot do VMware.

3. Replique a cópia do NetApp Snapshot, ou equivalente do snapshot, para um armazenamento alternativo.
4. Exclua o snapshot do VMware.

Você deve implementar um agendamento de backup usando essas tarefas para garantir que o dispositivo virtual do Unified Manager esteja protegido caso surjam problemas.

Para restaurar a VM, você pode usar o snapshot do VMware criado para restaurar a VM ao estado de backup do momento.

Backup e restauração usando um dump de banco de dados MySQL

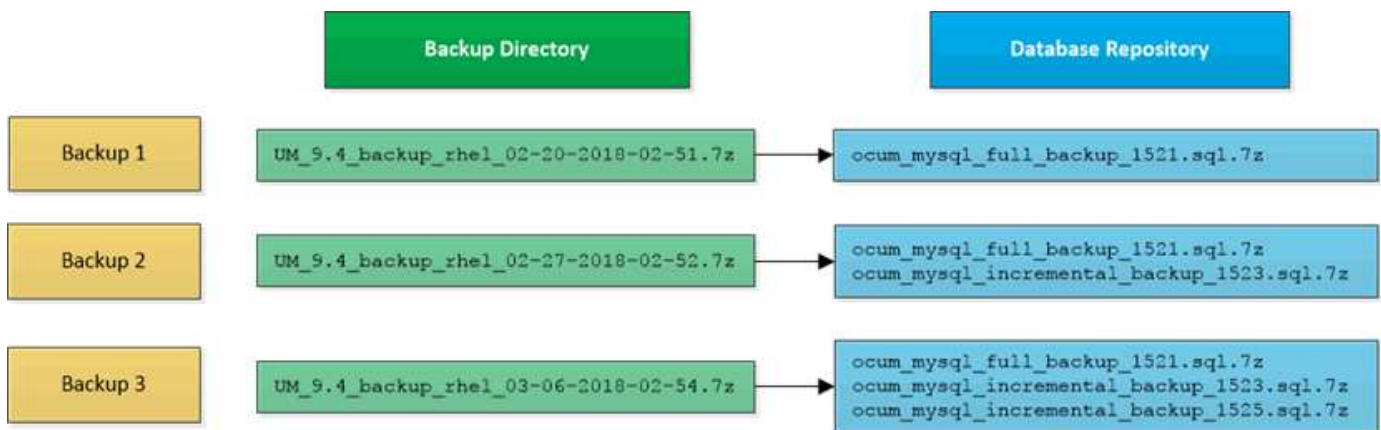
Um backup de despejo do banco de dados MySQL é uma cópia do banco de dados do Active IQ Unified Manager e dos arquivos de configuração que você pode usar em caso de falha do sistema ou perda de dados. Você pode agendar um backup para ser gravado em um destino local ou remoto. É altamente recomendável que você defina um local remoto externo ao sistema host do Active IQ Unified Manager .



O dump do 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 seus backups do MySQL estiverem demorando muitas horas para serem concluídos, você poderá fazer backup usando cópias de 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 do 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 do repositório do 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 do repositório do banco de dados. Na próxima vez que você gerar um backup, um único arquivo será criado no diretório de backup e um arquivo de backup incremental será criado no diretório do 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, conforme 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, deverá iniciar um processo para copiar os arquivos de backup para um local remoto para que eles estejam disponíveis caso tenha um problema no 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 e diretórios de backup necessários existem e são graváveis. Ele também verifica se há espaço suficiente no sistema para criar o arquivo de backup.

Configurar o destino e a programação para backups de despejo de banco de dados

Você pode configurar as definições de backup de despejo do banco de dados do Unified Manager para definir o caminho do backup do banco de dados, a contagem de retenção e o agendamento de backup. Você pode habilitar backups agendados diários ou semanais. Por padrão, os backups agendados estão desabilitados, mas você deve definir um agendamento de backup.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter no mínimo 150 GB de espaço disponível no local definido como caminho de backup.

É recomendável que você use 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, certifique-se de que as seguintes permissões e propriedades estejam definidas no diretório de backup.

Permissões: 0750, Propriedade: jboss:maintenance

- Quando o Unified Manager estiver instalado em um sistema Windows e usando o backup do MySQL, certifique-se de que somente o administrador tenha acesso ao diretório de backup.

É necessário mais tempo na primeira vez que um backup é executado do que nos backups subsequentes, porque o primeiro backup é um backup completo. Um backup completo pode ter mais de 1 GB e levar de três a quatro horas. Os 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, você pode fazer um backup completo periodicamente para substituir o backup antigo e seus arquivos incrementais. Como outra opção, você pode fazer um backup usando cópias instantâneas.
- O backup feito durante os primeiros 15 dias de adição de um novo cluster pode não ser preciso o suficiente para obter os dados históricos de desempenho.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Backup de banco de dados**.
2. Na página **Backup do banco de dados**, clique em **Configurações de backup**.
3. Configure os valores apropriados para um caminho de backup, contagem de retenção e agendamento.

O valor padrão para contagem de retenção é 10; você pode usar 0 para criar backups ilimitados.

4. Selecione o botão **Agendado diariamente** ou **Agendado semanalmente** e especifique os detalhes da programação.
5. Clique em **Aplicar**.

Os arquivos de backup de despejo do 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 existente do Unified Manager para o mesmo servidor Unified Manager ou para um servidor diferente. Você executa a operação de restauração no console de manutenção do Unified Manager.

Se você estiver executando uma operação de restauração no mesmo sistema (local) e todos os arquivos de backup estiverem armazenados localmente, você poderá executar a opção de restauração usando o local padrão. Se estiver executando uma operação de restauração em um sistema Unified Manager diferente (um sistema remoto), você deverá copiar o arquivo ou arquivos de backup 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. Você pode fazer login no sistema após a conclusão do processo de restauração.

Se você estiver restaurando a imagem de backup em 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 necessário, ao restaurar a imagem de backup em um novo servidor.



Arquivos de backup antigos não podem ser usados para restaurar uma imagem após 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 no Windows

Em caso de perda ou corrupção de dados, você pode usar o recurso de restauração para restaurar o Unified Manager ao estado estável anterior com perda mínima. Você pode restaurar o banco de dados MySQL do Unified Manager para um sistema Windows local ou remoto usando o console de manutenção do Unified Manager.

Antes de começar

- Você deve ter privilégios de 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 do banco de dados devem ser copiados para o `\database_dumps_repo` subdiretório sob o `\backup` diretório.

- Os arquivos de backup devem ser de `.7z` tipo.

O recurso de restauração é específico da plataforma e da versão. Você pode restaurar um backup do MySQL do Unified Manager somente na mesma versão do Unified Manager, e um backup do Windows só pode ser restaurado em uma plataforma Windows.



Se os nomes das pastas contiverem um espaço, você deverá incluir o caminho absoluto ou relativo do arquivo de backup entre aspas duplas.

Passos

1. Se você estiver executando uma restauração em um novo servidor, após instalar o Unified Manager, não inicie a interface do usuário nem configure nenhum cluster, usuário ou configuração de autenticação quando a instalação estiver concluída. O arquivo de backup preenche essas informações durante o processo de restauração.

2. Efetue login no sistema Unified Manager com credenciais de administrador.
3. Inicie o PowerShell ou o prompt de comando como administrador do Windows.
4. Digite o comando `maintenance_console` e pressione Enter.
5. No console de manutenção **Menu Principal**, insira o número da opção **Restauração de Backup**.
6. Digite o número do **Restaurar Backup do MySQL**.
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 poderá efetuar login no Unified Manager.

Após restaurar o backup, se o servidor OnCommand Workflow Automation não funcionar, execute as seguintes etapas:

1. No servidor de automação de fluxo de trabalho, 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.

Backup e restauração usando NetApp Snapshots

Uma cópia do NetApp Snapshot cria uma imagem pontual do banco de dados do Unified Manager e dos arquivos de configuração que você pode usar para restaurar em caso de falha do sistema ou perda de dados. Você agenda uma cópia do Snapshot para ser gravada em um volume em um dos seus clusters ONTAP periodicamente para que você sempre tenha uma cópia atualizada.



Esta funcionalidade não está disponível para o Active IQ Unified Manager instalado em um dispositivo virtual.

Configurar backup no Linux

Se o Active IQ Unified Manager estiver instalado em uma máquina Linux, você poderá decidir configurar seu backup e restauração usando o NetApp Snapshots.

As cópias de instantâneos levam muito pouco tempo, geralmente apenas alguns minutos, e o banco de dados do Unified Manager fica bloqueado por um período muito curto, portanto, há pouca interrupção na sua instalação. A imagem consome espaço de armazenamento mínimo e gera sobrecarga de desempenho insignificante porque registra apenas alterações nos arquivos desde que a última cópia do Snapshot foi feita. Como o Snapshot é criado em um cluster 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 executa uma verificação de integridade para verificar se o sistema de destino está disponível.



- Você pode restaurar uma cópia do Snapshot somente na mesma versão do Active IQ Unified Manager.

Por exemplo, se você criou um backup no Unified Manager 9.16, o backup poderá ser restaurado somente em sistemas Unified Manager 9.16.

- Se houver alguma alteração na configuração do Snapshot, isso poderá fazer com que o snapshot seja inválido.

Configurar local da cópia do instantâneo

Você pode configurar o volume onde as cópias do Snapshot serão armazenadas em um dos seus clusters ONTAP usando o ONTAP System Manager ou a CLI do ONTAP .

Antes de começar

O cluster, a VM de armazenamento e o volume devem atender aos seguintes requisitos:

- Requisitos do cluster:
 - ONTAP 9.3 ou superior deve ser instalado
 - Deve estar geograficamente próximo ao servidor do Unified Manager
 - Pode ser monitorado pelo Unified Manager, mas não é obrigatório
- Requisitos da VM de armazenamento:
 - A troca de nome e o mapeamento de nome devem ser definidos para usar “files”
 - Usuários locais criados para corresponder com usuários do lado do cliente
 - Certifique-se de que o acesso All Read/Write esteja selecionado
 - Certifique-se de que o acesso de superusuário esteja definido como “qualquer” na política de exportação
 - NFS para NetApp Snapshot para Linux
 - O NFSv4 deve ser habilitado no servidor NFS e no domínio de ID do NFSv4 especificado no cliente e na VM de armazenamento
 - O volume deve ter 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 ter 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 snapshot local deve ser desabilitada
 - O dimensionamento automático do volume deve ser habilitado
 - O nível de serviço de desempenho deve ser definido para uma política com alto IOPS e baixa latência, como “Extremo”

Para obter etapas detalhadas para criar o volume NFS, consulte ["Como configurar o NFSv4 no ONTAP 9"](#) e o ["Guia de configuração expressa do ONTAP 9 NFS"](#) .

Especifique o local de destino para cópias do Snapshot

Você deve configurar o local de destino para cópias do Active IQ Unified Manager Snapshot em um volume que você já configurou em um dos seus clusters ONTAP . Você deve usar o console de manutenção para definir o local.

- Você deve ter as credenciais de usuário root para o host Linux no qual o Active IQ Unified Manager está instalado.
- Você deve ter um ID de usuário e uma senha autorizados para efetuar login no console de manutenção do servidor do Unified Manager.
- Você deve ter o endereço IP de gerenciamento do cluster, o nome da VM de armazenamento, o nome do volume e o nome de usuário e a senha do sistema de armazenamento.
- Você deve ter montado o volume no host do Active IQ Unified Manager e deve ter o caminho de montagem.

Passos

1. Use o Secure Shell para se conectar ao endereço IP ou FQDN do sistema Active IQ Unified Manager .
2. Efetue login no sistema com o nome de usuário de manutenção (umadmin) e a senha.
3. Digite o comando `maintenance_console` e pressione Enter.
4. No console de manutenção **Menu Principal**, insira o número da opção **Restauração de Backup**.
5. Digite o número para *Configurar backup de instantâneo do NetApp *.
6. Digite o número para configurar o NFS.
7. Revise as informações que você precisará fornecer e insira o número para **Inserir detalhes da configuração de backup**.
8. Para identificar o volume onde o Snapshot 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 de usuário e a senha do sistema de armazenamento e o caminho de montagem.
9. Verifique essas informações e insira `y` .

O sistema executa as seguintes tarefas:

- Estabelece a conexão com o cluster
 - Interrompe todos os serviços
 - Cria um novo diretório no volume e copia os arquivos de configuração do banco de dados do Active IQ Unified Manager
 - Exclui os arquivos do Active IQ Unified Manager e cria um link simbólico para o novo diretório do 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 do Snapshot, caso ainda não tenha feito isso.

Configurar backup no Windows

O Active IQ Unified Manager oferece suporte a backup e restauração usando NetApp Snapshots no sistema operacional Windows com a ajuda de LUN usando o protocolo iSCSI.

O backup baseado em instantâneo 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 que impede qualquer gravação simultânea. Para que seu sistema Unified Manager instalado no sistema operacional Windows execute backup e restauração usando o NetApp Snapshots, você deve primeiro configurar o backup do Unified Manager para Snapshot usando o console de manutenção.

Antes de configurar o Unified Manager para criar cópias de Snapshot, você deve executar as seguintes tarefas de configuração.

- Configurar cluster ONTAP
- Configurar máquina host do Windows

Configurar local de backup para Windows

Você deve configurar o volume para armazenar cópias do Snapshot após fazer backup do Unified Manager no Windows.

Antes de começar

O cluster, a VM de armazenamento e o volume devem atender aos seguintes requisitos:

- Requisitos do cluster:
 - ONTAP 9.3 ou superior deve ser instalado
 - Deve estar geograficamente próximo ao servidor do Unified Manager
 - É monitorado pelo Unified Manager
- Requisitos da VM de armazenamento:
 - Conectividade iSCSI no cluster ONTAP
 - O protocolo iSCSI deve estar habilitado para a máquina configurada
 - Você deve ter um volume e LUN dedicados para configuração de backup. O volume selecionado deve conter apenas um LUN e nada mais.
 - O tamanho do LUN deve ser pelo menos duas vezes o tamanho dos dados esperados para serem manipulados no 9.9 Active IQ Unified Manager.

Isso também define o mesmo requisito de tamanho para o volume.

- Certifique-se de que o acesso All Read/Write esteja selecionado
 - Certifique-se de que o acesso de superusuário esteja definido como “qualquer” na política de exportação
- Requisitos de volume e LUN:
 - O volume deve ter pelo menos o dobro do tamanho do diretório de dados MySQL do Unified Manager.
 - O estilo de segurança deve ser definido como Windows
 - A política de snapshot local deve ser desabilitada
 - O dimensionamento automático do volume deve ser habilitado
 - O nível de serviço de desempenho deve ser definido para uma política com alto IOPS e baixa latência, como “Extremo”

Configurar cluster ONTAP

Você precisa executar algumas etapas de pré-configuração em clusters ONTAP antes de poder fazer backup e restaurar o Active IQ Unified Manager usando a cópia de instantâneo em sistemas Windows.

Você pode configurar o cluster ONTAP usando o prompt de comando ou a interface de usuário do System Manager. A configuração do cluster ONTAP envolve a configuração de LIFs de dados para que fiquem 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 de usuário do System Manager. Você precisará configurar uma rota de rede estática para esta VM de armazenamento para controlar como os LIFs usam a rede para 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 duas vezes o tamanho dos dados que o Active IQ Unified Manager espera manipular.

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 apropriada e um único LUN interno, garantindo que o volume seja dedicado somente para esse LUN.



Em um cenário em que o LUN é criado no Gerenciador do Sistema, desmapear o LUN pode excluir o igroup 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 for desmapeado.

4. Configure um grupo de iniciadores na VM de armazenamento.
5. Configurar um conjunto de portas.
6. Integre o igroup com o portset.
7. Mapeie o LUN para o igroup.

Configurar máquina host do Windows

Você precisa configurar sua máquina host Windows antes de poder usar o NetApp Snapshot para fazer backup e restaurar o Active IQ Unified Manager. Para iniciar o iniciador iSCSI da Microsoft em uma máquina host 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 solicitada uma confirmação e, após a confirmação, a caixa de diálogo Propriedades do iSCSI será exibida. Se for uma instalação existente do Windows, a caixa de diálogo Propriedades do iSCSI será exibida com um destino

inativo ou tentando se conectar. Portanto, você precisará garantir que todas as configurações anteriores no host 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 multicaminho 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.

Especifique o local de destino para cópias de instantâneo no Windows

Você deve configurar o local de destino para cópias do Active IQ Unified Manager Snapshot em um volume que você já configurou em um dos seus clusters ONTAP . Você deve usar o console de manutenção para definir o local.

- Você deve ter privilégios de administrador para o host Windows no qual o Active IQ Unified Manager está instalado.
- Você deve ter um ID de usuário e uma senha autorizados para efetuar login no console de manutenção do servidor do Unified Manager.
- Você deve ter o endereço IP de gerenciamento do 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 no host do 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. Efetue login no sistema com o nome de usuário de manutenção (umadmin) e a senha.
3. Digite o comando `maintenance_console` e pressione Enter.
4. No console de manutenção **Menu Principal**, insira o número da opção **Restauração de Backup**.
5. Digite o número para *Configurar backup de instantâneo do NetApp *.
6. Digite o número para configurar o iSCSI.
7. Revise as informações que você precisará fornecer e insira o número para **Inserir detalhes da configuração de backup**.
8. Para identificar o volume onde o Snapshot 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 de usuário e a senha do sistema de armazenamento e a unidade de montagem.
9. Verifique essas informações e insira `y` .

O sistema executa as seguintes tarefas:

- A VM de armazenamento é validada

- O volume é validado
- A unidade de montagem e o status são validados
- Existência e status do LUN
- Existência de unidade de rede
- A existência de espaço recomendado (mais que o dobro do diretório de dados mysql) no volume montado é validada
- Caminho LUN correspondente ao LUN dedicado no volume
- nome do igroup
- GUID do volume onde a unidade de rede está montada
- Iniciador iSCSI usado para comunicação com ONTAP

10. Saia do console de manutenção e inicie a interface do Active IQ Unified Manager para criar um agendamento para cópias do Snapshot.

Configurar backup por cópia instantânea do console de manutenção

Para fazer backup do Active IQ Unified Manager usando a cópia de instantâneo, você deve executar algumas etapas de configuração no console de manutenção.

Antes de começar

Você deve ter os seguintes detalhes para seu sistema:

- Endereço IP do cluster
- Nome do VM de armazenamento
- Nome do volume
- Nome da LUN
- Caminho de montagem
- Credenciais do sistema de armazenamento

Passos

1. Acesse o console de manutenção do Unified Manager.
2. Digite 4 para selecionar **Restauração de backup**.
3. Digite 2 para selecionar **Backup e restauração usando NetApp Snapshot**.



Se você quiser alterar a configuração de backup, digite 3 para selecionar *Atualizar configuração de backup de instantâneo do NetApp *. Você só pode atualizar a senha.

4. No menu, digite 1 para selecionar *Configurar backup de instantâneo do NetApp *.
5. Digite 1 para fornecer as informações necessárias.
6. Forneça o nome de usuário e a senha para o console de manutenção e, em seguida, forneça a confirmação de que o LUN está montado no host.

O processo então verifica se o diretório de dados, o caminho do 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 ocorrem em segundo plano são:

- Os serviços estão parados
- 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 NetApp Snapshot e refletido na interface do usuário como Backup de banco de dados (baseado em instantâneo).

Antes de iniciar uma operação de backup, você deve verificar se há alguma alteração na configuração do Snapshot, pois isso pode fazer com que o snapshot seja inválido. Suponha que você configurou o backup na unidade G e tirou um instantâneo. Mais tarde, você reconfigurou o backup para a unidade E e os dados foram salvos na unidade E de acordo com a nova configuração. Se você tentar restaurar o Snapshot tirado enquanto ele estava na unidade G, ele falhará e exibirá o erro de que a unidade G não existe.

Definir um agendamento de backup para Linux e Windows

Você pode configurar o agendamento no qual as cópias do Unified Manager Snapshot são criadas usando a interface do usuário do Unified Manager.

Antes de começar

- Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado as definições para criar cópias de snapshots no console de manutenção para identificar o destino onde os snapshots serão criados.

Cópias de instantâneos são criadas em apenas alguns minutos e o banco de dados do Unified Manager fica bloqueado apenas por alguns segundos.



O backup feito durante os primeiros 15 dias de adição de um novo cluster pode não ser preciso o suficiente para obter os dados históricos de desempenho.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Backup de banco de dados**.
2. Na página **Backup do banco de dados**, clique em **Configurações de backup**.
3. Insira o número máximo de cópias do Snapshot que você deseja reter no campo **Contagem de retenção**.

O valor padrão para contagem de retenção é 10. O número máximo de cópias do 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 **Agendado diariamente** ou **Agendado semanalmente** e especifique os detalhes da programação.
5. Clique em **Aplicar**.

Cópias instantâneas são criadas com base na programação. Você pode ver os arquivos de backup disponíveis na página Backup do banco de dados.

Devido à importância deste volume e dos instantâneos, você pode querer criar um ou dois alertas para este volume para ser notificado quando:

- O espaço do volume está 90% cheio. Use o evento **Volume Space Full** para configurar o alerta.

Você pode adicionar capacidade ao volume usando o ONTAP System Manager ou o ONTAP CLI 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 de instantâneos** para configurar o alerta.

Você pode excluir snapshots mais antigos usando o ONTAP System Manager ou o ONTAP CLI para que sempre haja espaço para novas cópias de snapshots.

Você configura alertas na página Configuração de alertas.

Restaurar o Unified Manager usando cópias de instantâneo

Caso ocorra perda ou corrupção de dados, você pode restaurar o Unified Manager ao estado estável anterior com perda mínima de dados. Você pode restaurar o banco de dados do Unified Manager Snapshot para um sistema operacional local ou remoto usando o console de manutenção do Unified Manager.

Antes de começar

- Você deve ter credenciais de usuário root para o host Linux e privilégios administrativos para a máquina host Windows na qual o Unified Manager está instalado.
- Você deve ter um ID de usuário e uma senha autorizados para efetuar login no console de manutenção do servidor do Unified Manager.

O recurso de restauração é específico da plataforma e 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. Efetue login no sistema com as credenciais de usuário root.
3. Digite o comando `maintenance_console` e pressione Enter.
4. No console de manutenção **Menu Principal**, digite 4 para a opção **Restauração de Backup**.
5. Digite 2 para selecionar **Backup e restauração usando NetApp Snapshot**.

Se você estiver executando uma restauração em um novo servidor, após instalar o Unified Manager, não inicie a interface do usuário nem configure nenhum cluster, usuário ou configuração de autenticação quando a instalação estiver concluída. Digite 1 para selecionar ***Configurar backup de instantâneo do NetApp *** e defina as configurações para cópias de instantâneo como estão no sistema original.

6. Digite 3 para selecionar **Restaurar usando NetApp Snapshot**.
7. Selecione a cópia do Snapshot da qual você deseja restaurar o Unified Manager. Pressione **Enter**.
8. Após a conclusão do processo de restauração, faça login na interface do usuário do Unified Manager.

Após restaurar o backup, se o servidor de automação de fluxo de trabalho não funcionar, execute as seguintes etapas:

1. No servidor de automação de fluxo de trabalho, 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 backup

Se você quiser alterar o tipo de backup do seu sistema Active IQ Unified Manager, poderá usar as opções do console de manutenção. A opção ***Desconfigurar backup de instantâneo do NetApp*** permite que você retorne ao backup baseado em MySQL.

Antes de começar

Você deve ter um ID de usuário e uma senha autorizados para efetuar login no console de manutenção do servidor do Unified Manager.

Passos

1. Acesse o console de manutenção.
2. Selecione 4 no **Menu Principal** para backup e restauração.
3. Selecione 2 no **Menu de Backup e Restauração**.
4. Selecione 4 para **Desconfigurar NetApp Snapshot Backup**.

As ações executadas são exibidas, como interromper os serviços, quebrar o link simbólico, mover os dados do armazenamento para o diretório e, em seguida, iniciar os serviços novamente.

Após o método de backup ser modificado, o mecanismo de backup é alterado de cópia instantânea para backup padrão do MySQL. Essa alteração aparece na seção Backup do banco de dados das Configurações gerais.

Backup sob demanda para o 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 backup baseado em MySQL ou NetApp Snapshot.

Você pode executar backup sob demanda usando o botão **Fazer backup agora** na página Backup do banco de dados. O backup sob demanda não depende dos agendamentos que você configurou para o Active IQ Unified Manager.

Migrar um appliance 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:
 - Você deve ter a função de Operador, Administrador de Aplicativos 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 em "[Instalando o Unified Manager em sistemas Linux](#)".
 - A versão do Unified Manager neste servidor deve ser a mesma que a versão no dispositivo virtual do qual você está usando o arquivo de backup.
 - Não inicie a interface do usuário nem configure nenhum cluster, usuário ou configuração 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 root 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, em seguida, restaurar o backup do banco de dados para o novo sistema.

Passos

1. No dispositivo virtual, clique em **Gerenciamento > Backup do banco de dados**.
2. Na página **Backup do banco de dados**, clique em **Configurações de backup**.
3. Altere o caminho do backup para `/jail/support`.
4. Na seção Agendar, selecione **Agendado diariamente** e insira um horário alguns minutos após o horário 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 levar de três a quatro horas para ser concluído.

7. Efetue login como usuário root 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 do 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 interface de usuário 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 caminho `/jail/support` no sistema Linux.
- Reconfigure ambos os lados da sua conexão de automação de fluxo de trabalho, se o WFA estiver sendo usado.

- Reconfigure as configurações de autenticação SAML, se estiver usando SAML.

Depois de verificar se tudo está funcionando conforme o esperado no seu sistema Linux, você pode desligar e remover o dispositivo virtual do Unified Manager.

Gerenciar 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 dispara um alerta, o script é executado. Você pode carregar scripts personalizados e testar sua execução quando um alerta for gerado.

A capacidade de carregar scripts no Unified Manager e executá-los é habilitada por padrão. Se sua organização não quiser permitir essa funcionalidade por motivos de segurança, você pode desabilitá-la em **Gerenciamento de armazenamento > Configurações de recursos**.

Como os scripts funcionam com alertas

Você pode associar um alerta ao seu script para que ele 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 tiver associado um alerta a um script, o script será executado. Você pode obter os detalhes dos argumentos passados ao script no 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 executadas com base no seu script personalizado para esse tipo de evento, e as ações **Corrigir** 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 reunir 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
```

Adicionar scripts

Você pode adicionar scripts no Unified Manager e associá-los a alertas. Esses scripts são executados automaticamente quando um alerta é gerado e permitem que você obtenha 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, o Perl deve ser instalado no servidor Unified Manager. Para instalações do VMware, o Perl 5 é instalado por padrão e os scripts suportarão 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 seu script criar arquivos de log para rastrear o progresso do script de alerta, você deverá garantir que os arquivos de log não sejam criados em nenhum lugar dentro da pasta de instalação do Unified Manager.

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode carregar scripts personalizados e coletar detalhes do evento sobre o alerta.



Se você não vir esse recurso disponível na interface do usuário, é porque a funcionalidade foi desabilitada pelo seu administrador. Se necessário, você pode habilitar essa funcionalidade em **Gerenciamento de armazenamento > Configurações de recursos**.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Scripts**.
2. Na página **Scripts**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar script**, clique em **Procurar** para selecionar seu arquivo de script.
4. Insira uma descrição para o script que você selecionar.
5. Clique em **Adicionar**.

Excluir scripts

Você pode excluir um script do Unified Manager quando ele não for mais necessário ou válido.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- O script não deve ser 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 você deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

Execução do script de teste

Você pode verificar se seu script é executado corretamente quando um alerta é gerado para um objeto de armazenamento.

- Você deve ter a função de Administrador de Aplicativos 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...
Adicionar um alerta	a. Clique em Adicionar. b. Na seção Ações, associe o alerta ao seu script de teste.
Editar um alerta	a. Selecione um alerta e clique em Editar. b. Na seção Ações, associe o alerta ao seu script de teste.

5. Clique em **Salvar**.
6. Na página **Configuração de alerta**, selecione o alerta que você adicionou ou modificou e clique em **Testar**.

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.

Gerenciar e monitorar grupos

Você pode criar grupos no Unified Manager para gerenciar objetos de armazenamento.

Entenda os grupos

Você pode criar grupos no Unified Manager para gerenciar objetos de armazenamento. 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 armazenamento heterogêneos (clusters, SVMs ou volumes). Você pode criar grupos no Unified Manager para gerenciar facilmente um conjunto de objetos de armazenamento. Os membros de um grupo podem mudar, dependendo dos objetos de armazenamento monitorados pelo Unified Manager em um determinado momento.

- Cada grupo tem um nome único.
- Você deve configurar no mínimo 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 armazenamento, como clusters, SVMs ou volumes.
- Objetos de armazenamento 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 ações simultaneamente em todos os objetos de armazenamento 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 regras de grupo para um grupo.

- Você deve associar uma regra de grupo a um grupo.
- Você deve associar um tipo de objeto a uma regra de grupo; somente um tipo de objeto é 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 condições, e cada grupo de condições pode ter uma ou mais condições.
- Os objetos de armazenamento podem pertencer a vários grupos com base nas regras de grupo que você criar.

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 condições 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 AND lógico. Todas as condições em um grupo de condições devem ser atendidas. Quando você cria ou modifica uma regra de grupo, é criada uma condição que aplica, seleciona e agrupa somente os objetos de armazenamento que atendem a todas as condições no grupo de condições. Você pode usar várias condições dentro de 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 operadores e especificando o valor necessário.

Tipo de objeto de armazenamento	Operandos aplicáveis
Volume	• Nome do objeto • Nome do cluster proprietário • Possuir nome SVM • Anotações
SVM	• Nome do objeto • Nome do cluster proprietário • Anotações
Conjunto	• Nome do objeto • Anotações

Quando você seleciona anotação como um operando para qualquer objeto de armazenamento, o operador “Is” fica 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 proprietário e as anotações que você define 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 “Contains”.

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 ao valor fornecido para o operando selecionado
- O valor do operando contém o valor fornecido para o operando selecionado
- Valor

O campo de valor muda com base no operando selecionado.

Exemplo de uma regra de grupo com condições

Considere um grupo de condições para um volume com as duas condições a seguir:

- O nome contém “vol”
- O nome do SVM é “data_svm”

Este grupo de condições seleciona todos os volumes que incluem “vol” em seus nomes e que estão hospedados em SVMs com o nome “data_svm”.

Grupos de condições

Grupos de condições são executados usando OR lógico e depois aplicados a objetos de armazenamento. Os objetos de armazenamento devem satisfazer um dos grupos de condições para 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 de objetos de armazenamento a serem incluídos em um grupo.

Exemplo de uma regra de grupo com grupos de condições

Considere dois grupos de condições para um volume, com cada grupo contendo as duas condições a seguir:

- Grupo de condição 1
 - O nome contém “vol”
 - O nome do SVM é “data_svm”. O grupo de condições 1 seleciona todos os volumes que incluem “vol” em seus nomes e que estão hospedados em SVMs com o nome “data_svm”.
- Grupo de condição 2
 - O nome contém “vol”
 - O valor de anotação de data-priority é “crítico”. O grupo de condições 2 seleciona todos os volumes que incluem “vol” em seus nomes e que são anotados com o valor de anotação de data-priority 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 estão 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 “critical”.

Como as ações de grupo funcionam em objetos de armazenamento

Uma ação de grupo é uma operação executada em todos os objetos de armazenamento em um grupo. Por exemplo, você pode configurar a ação do grupo de limite de volume para alterar simultaneamente os valores de limite de volume de todos os volumes em um grupo.

Os grupos oferecem suporte a tipos exclusivos de ações de grupo. 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 exclusivas

Considere um volume A que pertence aos grupos G1 e G2, e as seguintes ações de grupo de limite de integridade de volume são 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 de Snapshot do volume

O `Change_capacity_threshold` a ação do 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 o `Change_capacity_threshold` ação em grupo. Não é possível configurar outro tipo de limite de volume de ação de grupo para o grupo G1 ou G2.

Adicionar grupos

Você pode criar grupos para combinar clusters, volumes e máquinas virtuais de armazenamento (SVMs) para facilitar o gerenciamento.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode definir regras de grupo para adicionar ou remover membros do grupo e modificar ações do grupo.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Grupos**.
2. Na aba **Grupos**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar grupo**, insira um nome e uma descrição para o grupo.
4. Clique em **Adicionar**.

Editar grupos

Você pode editar o nome e a descrição de um grupo criado no Unified Manager.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Ao editar um grupo para atualizar o nome, você deve especificar um nome exclusivo; não é possível usar um nome de grupo existente.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Grupos**.
2. Na aba **Grupos**, selecione o grupo que você deseja editar e clique em **Editar**.
3. Na caixa de diálogo **Editar grupo**, altere o nome, a descrição ou ambos do grupo.
4. Clique em **Salvar**.

Excluir grupos

Você pode excluir um grupo do Unified Manager quando ele não for mais necessário.

Antes de começar

- Nenhum dos objetos de armazenamento (clusters, SVMs ou volumes) deve estar associado a nenhuma regra de grupo associada ao grupo que você deseja excluir.
- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Grupos**.
2. Na aba **Grupos**, selecione o grupo que você deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

Excluir um grupo não exclui as ações de grupo associadas a ele. No entanto, essas ações de grupo não serão mapeadas depois que o grupo for excluído.

Adicionar regras de grupo

Você pode criar regras de grupo para um grupo adicionar dinamicamente objetos de armazenamento, 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

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Os objetos de armazenamento que estão sendo monitorados no momento são adicionados assim que a regra de grupo é criada. Novos objetos são adicionados somente após a conclusão do ciclo de monitoramento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Grupos**.
2. Na aba **Regras do Grupo**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar regra de grupo**, especifique um nome para a regra de grupo.
4. No campo **Tipo de objeto de destino**, selecione o tipo de objeto de armazenamento que você deseja agrupar.
5. No campo **Grupo**, selecione o grupo necessário para o qual você deseja criar regras de grupo.
6. Na seção **Condições**, execute as seguintes etapas para criar uma condição, um grupo de condições ou

ambos:

Para criar....	Faça isso...
Uma condição	a. Selecione um operando da lista de operandos. b. Selecione Contém ou É como operador. c. Insira um valor ou selecione um valor na lista disponível.
Um grupo de condições	a. Clique em Adicionar Grupo de Condições b. Selecione um operando da lista de operandos. c. Selecione Contém ou É como operador. d. Insira um valor ou selecione um valor na lista disponível. e. Clique em Adicionar condição para criar mais condições, se necessário, e repita as etapas de a a d para cada condição.

7. Clique em **Adicionar**.

Exemplo para criar uma regra de grupo

Execute as seguintes etapas 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

1. Especifique um nome para a regra de grupo.
2. Selecione o tipo de objeto como máquina virtual de armazenamento (SVM).
3. Selecione um grupo da lista de grupos.
4. Na seção Condições, selecione **Nome do Objeto** como operando.
5. Selecione **Contém** como operador.
6. Insira o valor como `svm_data`.
7. Clique em **Adicionar grupo de condições**.
8. Selecione **Nome do Objeto** como operando.
9. Selecione **Contém** como operador.
10. Insira o valor como `vol`.
11. Clique em **Adicionar condição**.
12. Repita as etapas 8 a 10 selecionando **data-priority** como o operando na etapa 8, **Is** como o operador na etapa 9 e **critical** como o valor na etapa 10.
13. Clique em **Adicionar** para criar a condição para a regra de grupo.

Editar regras do grupo

Você pode editar regras de grupo para modificar os grupos de condições 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

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Grupos**.
2. Na aba **Regras de Grupo**, selecione a regra de grupo que você 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 condições e as condições conforme necessário.



Não é possível alterar o tipo de objeto de destino para uma regra de grupo.

4. Clique em **Salvar**.

Excluir regras de grupo

Você pode excluir uma regra de grupo do Active IQ Unified Manager quando ela não for mais necessária.

Antes de começar

Você deve ter a função de Administrador de Aplicativos 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 aba **Regras de Grupo**, selecione a regra de grupo que você deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

Adicionar ações de grupo

Você pode configurar ações de grupo que deseja aplicar a objetos de armazenamento em um grupo. Configurar ações para um grupo permite economizar tempo, porque você não precisa adicionar essas ações a cada objeto individualmente.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Grupos**.
2. Na aba **Ações de Grupo**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar ação de grupo**, insira um nome e uma descrição para a ação.
4. No menu **Grupo**, selecione um grupo para o qual você deseja configurar a ação.
5. No menu **Tipo de ação**, selecione um tipo de ação.

A caixa de diálogo se expande, permitindo que você configure o tipo de ação selecionado com os

parâmetros necessários.

6. Insira valores apropriados para os parâmetros necessários para configurar uma ação de grupo.
7. Clique em **Adicionar**.

Editar ações do grupo

Você pode editar os parâmetros de ação do grupo configurados no Unified Manager, como o nome da ação do grupo, a descrição, o nome do grupo associado e os parâmetros do tipo de ação.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Grupos**.
2. Na aba **Ações de Grupo**, selecione a ação de grupo que você deseja editar e clique em **Editar**.
3. Na caixa de diálogo **Editar ação de grupo**, altere o nome da ação do grupo, a descrição, o nome do grupo associado e os parâmetros do tipo de ação, conforme necessário.
4. Clique em **Salvar**.

Configurar limites de integridade de volume para grupos

Você pode configurar limites de integridade de volume em nível de grupo para capacidade, cópias de instantâneo, cotas de qtree, crescimento e inodes.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

O tipo de ação de grupo de limite de integridade do volume é aplicado somente aos volumes de um grupo.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Grupos**.
2. Na aba **Ações de Grupo**, clique em **Adicionar**.
3. Insira um nome e uma descrição para a ação do grupo.
4. Na caixa suspensa **Grupo**, selecione um grupo para o qual você deseja configurar a ação do grupo.
5. Selecione **Tipo de ação** como limite de integridade do volume.
6. Selecione a categoria para a qual você deseja definir o limite.
7. Insira os valores necessários para o limite de saúde.
8. Clique em **Adicionar**.

Excluir ações de grupo

Você pode excluir uma ação de grupo do Unified Manager quando ela não for mais necessária.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Quando você exclui a ação de grupo para o limite de integridade do volume, limites globais são aplicados aos objetos de armazenamento nesse grupo. Nenhum limite de integridade no nível do objeto definido no objeto de armazenamento será afetado.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Grupos**.
2. Na aba **Ações de grupo**, selecione a ação de grupo que você 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 serão aplicadas aos objetos de armazenamento em um grupo. 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 de grupo dependendo de suas necessidades.

Antes de começar

Você deve ter a função de Administrador de Aplicativos 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 do grupo. No entanto, você deve salvar as alterações para que a repriorização seja refletida na grade de ações do grupo.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Grupos**.
2. Na aba **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**.

Priorizar eventos de objetos de armazenamento usando anotações

Você pode criar e aplicar regras de anotação a objetos de armazenamento para poder identificar e filtrar esses objetos com base no tipo de anotação aplicada e sua prioridade.

Entenda mais sobre anotações

Entender os conceitos sobre anotações ajuda você a gerenciar os eventos relacionados aos objetos de armazenamento em seu ambiente.

O que são anotações

Uma anotação é uma sequência de texto (o nome) que é atribuída a outra sequência de texto (o valor). Cada par nome-valor de anotação pode ser associado dinamicamente a objetos de armazenamento usando regras de anotação. Ao associar objetos de armazenamento a anotações predefinidas, você pode filtrar e visualizar os eventos

relacionados a eles. Você pode aplicar anotações a clusters, volumes e máquinas virtuais de armazenamento (SVMs).

Cada nome de anotação pode ter vários valores; cada par nome-valor pode ser associado a um objeto de armazenamento por meio de regras.

Por exemplo, você pode criar uma anotação chamada “data-center” com os valores “Boston” e “Canada”. 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 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 funcionam as regras de anotação 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)). Você pode usar grupos de condições ou condições para definir regras de anotação.

- Você deve associar uma regra de anotação a uma anotação.
- Você deve associar um tipo de objeto a uma regra de anotação; somente 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. Você pode aplicar todos os grupos de condições definidos em uma regra de anotação para anotar objetos de armazenamento.

As condições dentro de um grupo de condições são executadas usando AND lógico. Todas as condições em um grupo de condições devem ser atendidas. Quando você cria ou modifica uma regra de anotação, é criada uma condição que aplica, seleciona e anota somente os objetos de armazenamento que atendem a todas as condições no grupo de condições. 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 operadores e especificando o valor necessário.

Tipo de objeto de armazenamento	Operandos aplicáveis
Volume	• Nome do objeto • Nome do cluster proprietário • Possuir nome SVM • Anotações

Tipo de objeto de armazenamento	Operandos aplicáveis
SVM	• Nome do objeto • Nome do cluster proprietário • Anotações
Conjunto	• Nome do objeto • Anotações

Quando você seleciona anotação como um operando para qualquer objeto de armazenamento, o operador “Is” fica 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 ao 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 condições a seguir:

- O nome contém “vol”
- O nome do SVM é “data_svm”

Esta regra de anotação anota todos os volumes que incluem “vol” em seus nomes e que estão hospedados em SVMs com o nome “data_svm” com a anotação selecionada e o tipo de anotação.

Grupos de condições

Grupos de condições são executados usando OR lógico e depois 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 duas condições a seguir:

- Grupo de condição 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 estão hospedados em SVMs com o nome “data_svm”.
- Grupo de condição 2
 - O nome contém “vol”

- O valor de anotação de data-priority é “critical”. Este grupo de condições anota todos os volumes que incluem “vol” em seus nomes e que são anotados com o valor de anotação data-priority como “critical”.

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 estão 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 Crítico de missão, Alto e Baixo. Esses valores permitem que você anote objetos de armazenamento com base na prioridade dos dados que eles contêm. Você não pode editar ou excluir 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 aplicativos 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, objetos que estão no armazenamento secundário, como destinos de backup e espelho, podem ter 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 aos objetos de armazenamento.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na página **Anotações**, clique em **Adicionar anotação**.
3. Na caixa de diálogo **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 às anotações

Você pode adicionar valores às anotações e, em seguida, associar objetos de armazenamento a um par nome-valor de anotação específico. Adicionar valores às anotações ajuda você a gerenciar objetos de armazenamento de forma mais eficaz.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você não pode 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 **Adicionar** na seção **Valores**.
3. Na caixa de diálogo **Adicionar valor de anotação**, especifique um valor para a anotação.

O valor especificado deve ser exclusivo para a anotação selecionada.

4. Clique em **Adicionar**.

Excluir anotações

Você pode excluir anotações personalizadas e seus valores quando eles não forem mais necessários.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Os valores de anotação não devem ser usados em outras anotações ou regras de grupo.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na aba **Anotações**, selecione a anotação que você deseja excluir.

Os detalhes da anotação selecionada são exibidos.

3. Clique em **Ações > Excluir** para excluir a anotação selecionada e seu valor.
4. Na caixa de diálogo de aviso, clique em **Sim** para confirmar a exclusão.

Veja a lista de anotações e detalhes

Você pode visualizar a lista de anotações que são dinamicamente associadas a clusters, volumes e máquinas virtuais de armazenamento (SVMs). Você também pode visualizar detalhes como a descrição, criado por, data de criação, valores, regras e os objetos associados à anotação.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na aba **Anotações**, clique no nome da anotação para visualizar os detalhes associados.

Excluir valores das anotações

Você pode excluir valores associados a anotações personalizadas quando esse valor não se aplicar mais à anotação.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- O valor da anotação não deve ser associado a nenhuma regra de anotação ou regra de grupo.

Você não pode excluir valores de anotações predefinidas.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na lista de anotações na aba **Anotações**, selecione a anotação da qual você deseja excluir 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 excluído e não é mais exibido na lista de valores da anotação selecionada.

Criar 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

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Os objetos de armazenamento que estão sendo monitorados no momento são anotados assim que a regra de anotação é criada. Novos objetos são anotados somente após a conclusão do ciclo de monitoramento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na aba **Regras de Anotação**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar regra de anotação**, especifique um nome para a regra de anotação.
4. No campo **Tipo de objeto de destino**, selecione o tipo de objeto de armazenamento que você deseja anotar.
5. Nos campos **Aplicar anotação**, selecione a anotação e o valor da anotação que você deseja usar.
6. Na seção **Condições**, execute a ação apropriada para criar uma condição, um grupo de condições ou ambos:

Para criar...	Faça isso...
Uma condição	a. Selecione um operando da lista de operandos. b. Selecione Contém ou É como operador. c. Insira um valor ou selecione um valor na lista disponível.
Um grupo de condições	a. Clique em Adicionar grupo de condições . b. Selecione um operando da lista de operandos. c. Selecione Contém ou É como operador. d. Insira um valor ou selecione um valor na lista disponível. e. Clique em Adicionar condição para criar mais condições, se necessário, e repita as etapas de a a d para cada condição.

7. Clique em **Adicionar**.

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 a configuração de uma condição e a adição de 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 armazenamento (SVM).
3. Selecione uma anotação na lista de anotações e especifique um valor.
4. Na seção Condições, selecione **Nome do Objeto** como operando.
5. Selecione **Contém** como operador.
6. Insira o valor como `svm_data`.
7. Clique em **Adicionar grupo de condições**.
8. Selecione **Nome do Objeto** como operando.
9. Selecione **Contém** como operador.
10. Insira o valor como `vol`.
11. Clique em **Adicionar condição**.
12. Repita as etapas 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 **Adicionar**.

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 pares nome-valor necessária para a

anotação.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. Navegue até os objetos de armazenamento que você deseja anotar:

Para adicionar anotações a...	Faça isso...
Aglomerados	a. Clique em Armazenamento > Clusters . b. Selecione um ou mais clusters.
Volumes	a. Clique em Armazenamento > Volumes . b. Selecione um ou mais volumes.
SVMs	a. Clique em Armazenamento > SVMs . b. Selecione uma ou mais SVMs.

2. Clique em **Anotar** e selecione um par nome-valor.
3. Clique em **Aplicar**.

Editar regras de anotação

Você pode editar regras de anotação para modificar os grupos de condições e as condições dentro do grupo de condições para adicionar ou remover anotações de objetos de armazenamento.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

As anotações são dissociadas dos 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 aba **Regras de anotação**, selecione a regra de anotação que deseja editar e clique em **Ações > Editar**.
3. Na caixa de diálogo **Editar regra de anotação**, altere o nome da regra, o nome e o valor da anotação, os grupos de condições e as condições, conforme necessário.

Não é possível alterar o tipo de objeto de destino 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

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na aba **Regras de Anotação**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar regra de anotação**, insira um nome para a regra.
4. Selecione um tipo de objeto na lista Tipo de objeto de destino e, em seguida, selecione um nome de anotação e um valor na lista.
5. Na seção **Condições** da caixa de diálogo, selecione um operando e um operador da 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. Insira um nome para a regra de anotação.
2. Selecione o tipo de objeto de destino como SVM.
3. Selecione uma anotação da lista de anotações e um valor.
4. No campo **Condições**, selecione **Nome do Objeto** como operando.
5. Selecione **Contém** como operador.
6. Insira o valor como `svm_data`.
7. Clique em **Adicionar**.

Excluir regras de anotação

Você pode excluir regras de anotação do Active IQ Unified Manager quando elas não forem mais necessárias.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Quando você exclui uma regra de anotação, a anotação é dissociada e removida dos objetos de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Anotações**.
2. Na aba **Regras de anotação**, selecione a regra de anotação que você 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 aos objetos de armazenamento. As regras de anotação são aplicadas aos objetos de armazenamento sequencialmente com base em sua classificação. Quando você configura uma regra de anotação, a classificação é a menor. Mas você pode alterar a classificação da regra de anotação dependendo de suas necessidades.

Antes de começar

Você deve ter a função de Administrador de Aplicativos 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 aba **Regras de Anotação**, clique em **Reordenar**.
3. Na caixa de diálogo **Reordenar regra de anotação**, arraste e solte uma ou várias linhas para reorganizar a sequência das regras de anotação.
4. Clique em **Salvar**.

Você deve salvar as alterações para que a reordenação seja exibida.

Envie um pacote de suporte por meio da interface 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 de AutoSupport fornece. Você pode enviar um pacote de suporte ao suporte técnico usando a interface de usuário 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 por vez.

Informações relacionadas

["Funções e recursos do usuário do Unified Manager"](#)

Enviar mensagens de AutoSupport e pacotes de suporte ao suporte técnico

A página AutoSupport permite que você envie mensagens de AutoSupport predefinidas e sob demanda para sua equipe de suporte técnico para garantir a operação correta do seu ambiente e ajudar você a manter a integridade do seu ambiente. O AutoSupport é habilitado por padrão e não deve ser desabilitado para que você receba os benefícios do NetAppActive IQ.

Você pode enviar informações de diagnóstico do sistema e dados detalhados sobre o servidor do Unified Manager em uma mensagem quando necessário, agendar o envio periódico de uma mensagem ou até

mesmo gerar e enviar pacotes de suporte para a equipe de suporte técnico.



Um usuário com função de administrador de armazenamento pode gerar e enviar mensagens de AutoSupport sob demanda e pacotes de suporte ao suporte técnico. No entanto, somente um administrador ou usuário de manutenção pode habilitar ou desabilitar o AutoSupport periódico e configurar as definições HTTP conforme descrito na seção Configurando o 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 de AutoSupport sob demanda e pacotes de suporte ao suporte técnico.

Enviar mensagens de AutoSupport sob demanda

Você pode gerar e enviar uma mensagem sob demanda para o suporte técnico, para um destinatário de e-mail específico ou para ambos.

Passos

1. Navegue até **Geral** > * AutoSupport* e execute uma ou ambas as seguintes ações:
2. Se você quiser enviar a mensagem do AutoSupport para o suporte técnico, marque a caixa de seleção **Enviar para o Suporte Técnico**.
3. Se você quiser enviar a mensagem do 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 **Gerar e Enviar AutoSupport**.

Habilitar AutoSupport periódico

Você pode enviar mensagens específicas e predefinidas ao suporte técnico para diagnóstico e resolução de problemas periodicamente. Esta funcionalidade é habilitada por padrão. Se desabilitado, um administrador ou usuário de manutenção pode habilitar as configurações.

Passos

1. Navegue até **Geral** > * AutoSupport*.
2. Na seção AutoSupport Periódico, marque a caixa de seleção **Habilitar envio periódico de dados de AutoSupport para o Active IQ**.
3. Se necessário, defina o nome, a porta e as informações de autenticação para o servidor proxy HTTP, conforme descrito na seção Configurando o servidor proxy HTTP.
4. Clique em **Salvar**.

Pacote de suporte sob demanda para upload

Você pode gerar e enviar um pacote de suporte ao suporte técnico com base na necessidade 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 do 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 logs e registros de banco de dados de configuração — ele 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 **Gerar e enviar pacote de suporte**.
3. Para enviar um pacote de suporte leve ao suporte técnico, no pop-up Gerar e enviar pacote de suporte, marque a caixa de seleção **Gerar pacote de suporte leve**.
4. Como alternativa, para enviar um pacote de suporte completo, marque a caixa de seleção **Gerar pacote de suporte completo**. Selecione os tipos de dados específicos a serem incluídos ou excluídos no pacote de suporte.



Mesmo que você não selecione nenhum tipo de dado, o pacote de suporte ainda será gerado com outros dados do Unified Manager.

5. Marque a caixa de seleção **Enviar o pacote para o suporte técnico** para gerar e enviar o pacote para o suporte técnico. Se você não marcar esta 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/ em sistemas Linux e em ProgramData\NetApp\OnCommandAppData\ocum\support em sistemas Windows.
6. Clique em **Enviar**.

Configurar servidor proxy HTTP

Você pode designar um proxy para fornecer acesso à Internet para enviar conteúdo do AutoSupport ao suporte caso seu ambiente não forneça acesso direto do servidor do Unified Manager. Esta seção está disponível apenas para usuários administradores e de manutenção.

• Usar proxy HTTP

Marque esta caixa para identificar o servidor que está sendo usado como proxy HTTP.

Digite o nome do host ou endereço IP do servidor proxy e o número da porta usada para conectar ao servidor.

• Usar autenticação

Marque esta caixa se precisar fornecer informações de autenticação para acessar o servidor que está sendo usado como proxy HTTP.

Digite o nome de usuário e a senha necessários para autenticação com o proxy HTTP.



Proxies HTTP que fornecem apenas Autenticação Básica não são suportados.

Acesse o console de manutenção

Se a interface do usuário do Unified Manager não estiver em operação ou se você precisar executar funções que não estão disponíveis na interface do usuário, você poderá acessar o console de manutenção para gerenciar seu sistema Unified Manager.

Antes de começar

Você deve ter instalado e configurado o Unified Manager.

Após 15 minutos de inatividade, o console de manutenção desconecta você.



Quando instalado no VMware, se você já tiver efetuado login como usuário de manutenção por meio do console do VMware, não será possível efetuar login simultaneamente usando o Secure Shell.

Etapa

1. Siga estas etapas para acessar o console de manutenção:

Neste sistema operacional...	Siga estes passos...
VMware	a. Usando o Secure Shell, conecte-se ao endereço IP ou ao nome de domínio totalmente qualificado do dispositivo virtual do Unified Manager. b. Efetue login no console de manutenção usando seu nome de usuário e senha de manutenção.
Linux	a. Usando o Secure Shell, conecte-se ao endereço IP ou ao nome de domínio totalmente qualificado do sistema Unified Manager. b. Efetue login no sistema com o nome de usuário de manutenção (umadmin) e a senha. c. Digite o comando <code>maintenance_console</code> e pressione Enter.
Windows	a. Efetue login no sistema Unified Manager com credenciais de administrador. b. Inicie o PowerShell como administrador do Windows. c. Digite o comando <code>maintenance_console</code> e pressione Enter.

O menu do console de manutenção do Unified Manager é exibido.

Gerar e carregar 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 seu servidor Unified Manager estiver conectado à Internet, você também poderá carregar o 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 do cluster ou levar muito tempo para serem concluídos, ao selecionar o pacote de suporte completo, você pode especificar os 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 logs e registros de banco de

dados de configuração — ele 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 **Gerar pacote de suporte leve** ou **Gerar pacote de suporte** dependendo do nível de detalhes que você deseja ter no pacote de suporte.
3. Se você escolher o pacote de suporte completo, selecione 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 servidor MySQL.

- **despejo de pilha**

Um instantâneo do estado dos principais processos do servidor do Unified Manager. Esta opção está desabilitada por padrão e deve ser selecionada somente quando solicitada pelo suporte ao cliente.

- **gravações de aquisição**

Uma 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. Tipo **g** e pressione Enter para gerar o pacote de suporte.

Como a geração de um pacote de suporte é uma operação que exige muita memória, você será solicitado a verificar se tem certeza de que deseja gerar o pacote de suporte neste momento.

5. Tipo **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 a especificar o período para o qual deseja que as estatísticas de desempenho sejam incluídas. Incluir estatísticas de desempenho pode levar muito tempo e espaço, então você também pode despejar o banco de dados sem incluir estatísticas de desempenho:

- a. Insira a data de início no formato AAAAMMDD.

Por exemplo, insira 20210101 para 1º de janeiro de 2021. Digitar **n** se você não quiser que estatísticas de desempenho sejam incluídas.

- b. Insira o número de dias de estatísticas a serem incluídos, começando às 00h da data de início especificada.

Você pode inserir um número de 1 a 10.

Se você estiver incluindo estatísticas de desempenho, o sistema exibirá o período de tempo durante o

qual as estatísticas de desempenho serão coletadas.

7. Após a criação do pacote de suporte, você será perguntado se deseja enviá-lo ao NetApp. Tipo y e pressione Enter.

Você será solicitado a inserir o número do seu caso de suporte.

8. Se você já tiver um número de caso, insira-o e pressione Enter. Caso contrário, basta pressionar Enter.

O pacote de suporte é carregado no NetApp.

Se o seu servidor 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 do 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 em ProgramData\NetApp\OnCommandAppData\ocum\support em sistemas Windows.

Informações relacionadas

["Funções e recursos do usuário do Unified Manager"](#)

Recupere 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 seu servidor do Unified Manager. Você pode enviar o pacote de suporte ao suporte técnico para 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 via 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 você 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 seu sistema local.

Recupere o pacote de suporte usando um cliente UNIX ou Linux

Se você for um usuário UNIX ou Linux, poderá recuperar o pacote de suporte do seu vApp usando a interface de linha de comando (CLI) no seu 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 via Telnet ou console, usando seu 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...	Então use o seguinte comando...
SCP	<code>scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>
SFTP	<code>sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>

O nome do pacote de suporte é fornecido quando você o gera usando o console de manutenção.

- 4. Digite a senha do usuário 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
```

Envie um pacote de suporte para o suporte técnico

Quando um problema exige diagnóstico mais detalhado e informações de solução de problemas do que uma mensagem do AutoSupport fornece, você pode enviar um pacote de suporte ao 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. Efetue login no site de suporte da NetApp .
2. Carregue o arquivo.

["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 ajudar você 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 e detalhes sobre volumes, máquinas virtuais de armazenamento (SVMs), agregados e assim por diante.

Componentes do cluster e por que eles podem estar em disputa

Você pode identificar problemas de desempenho do cluster quando um componente do cluster entra em contenção. O desempenho das cargas de trabalho que usam o componente fica lento 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 ter um desempenho ideal. Seu desempenho diminuiu, e o desempenho de outros componentes do cluster e cargas de trabalho, chamados de *vítimas*, podem ter aumentado a latência. Para tirar um componente da disputa, você deve reduzir sua carga de trabalho ou aumentar sua capacidade de lidar com mais trabalho, para que o desempenho possa retornar aos níveis normais. Como o Unified Manager coleta e analisa o desempenho da carga de trabalho em intervalos de cinco minutos, ele detecta apenas quando um componente do cluster é usado em excesso de forma consistente. Picos transitórios de uso excessivo que duram apenas um curto período dentro do intervalo de cinco minutos não são detectados.

Por exemplo, um agregado de armazenamento pode estar em disputa porque uma ou mais cargas de trabalho nele estão competindo para que suas solicitações de E/S sejam atendidas. Outras cargas de trabalho no agregado podem ser impactadas, causando diminuição de desempenho. Para reduzir a quantidade de atividade no agregado, há diferentes etapas que você pode seguir, como mover uma ou mais cargas de trabalho para um agregado ou nó menos ocupado, para diminuir a demanda geral de carga de trabalho no agregado atual. Para um grupo de políticas de QoS, você pode ajustar o limite de taxa de transferência ou mover cargas de trabalho para um grupo de políticas diferente, para que as cargas de trabalho não sejam mais limitadas.

O Unified Manager monitora os seguintes componentes do cluster para alertá-lo quando eles estão em

contenção:

- **Rede**

Representa o tempo de espera de solicitações de E/S pelos protocolos de rede externos no cluster. O tempo de espera é o tempo gasto esperando que as transações “transferência pronta” 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 afetando 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 nó que manipula o processamento da rede pode ter mudado 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 afetando a latência de uma ou mais cargas de trabalho.

Ao usar um cluster All SAN Array em uma configuração ativa-ativa, o valor de latência de processamento da rede é exibido para ambos os nós para que você possa verificar se os nós estão compartilhando a carga igualmente.

- **Limite Máximo de QoS**

Representa a configuração máxima (pico) de taxa de transferência do grupo de políticas de Qualidade de Serviço (QoS) de armazenamento atribuído à carga de trabalho. Se o componente do grupo de políticas estiver em contenção, isso significa que todas as cargas de trabalho no grupo de políticas estão sendo limitadas pelo limite de taxa de transferência definido, o que está impactando a latência de uma ou mais dessas cargas de trabalho.

- **Limite mínimo de QoS**

Representa a latência para uma carga de trabalho que está sendo causada pela configuração mínima (esperada) de taxa de transferência de QoS atribuída a outras cargas de trabalho. Se o QoS mínimo definido em determinadas cargas de trabalho usar a maior parte da largura de banda para garantir a taxa de transferência prometida, outras cargas de trabalho serão limitadas e terão mais latência.

- **Interconexão de Cluster**

Representa os cabos e adaptadores com os quais os nós agrupados estão fisicamente conectados. Se o componente de interconexão do cluster estiver em contenção, isso significa que o alto tempo de espera para solicitações de E/S na interconexão do cluster está afetando a latência de uma ou mais cargas de trabalho.

- *** Data Processing***

Representa o componente de software no cluster envolvido com o processamento de E/S entre o cluster e o agregado de armazenamento que contém a carga de trabalho. O nó que manipula o processamento de dados pode ter mudado desde que o evento foi detectado. Se o componente de processamento de dados estiver em contenção, isso significa que a alta utilização no nó de processamento de dados está afetando a latência de uma ou mais cargas de trabalho.

- **Ativação de Volume**

Representa o processo que rastreia o uso de todos os volumes ativos. Em ambientes grandes onde mais de 1000 volumes estão ativos, esse processo rastreia quantos volumes críticos precisam acessar recursos

por meio do nó ao mesmo tempo. Quando o número de volumes ativos simultâneos excede o limite máximo recomendado, alguns dos volumes não críticos sofrerão latência, conforme identificado aqui.

- *** Recursos do MetroCluster ***

Representa os recursos do MetroCluster , incluindo NVRAM e links entre switches (ISLs), usados para espelhar dados entre clusters em uma configuração do MetroCluster . Se o componente MetroCluster estiver em contenção, isso significa que há alta taxa de transferência de gravação de cargas de trabalho no cluster local ou um problema de integridade do link que está afetando a latência de uma ou mais cargas de trabalho no cluster local. Se o cluster não estiver em uma configuração MetroCluster , este ícone não será exibido.

- **Operações agregadas ou SSD agregadas**

Representa o agregado de armazenamento no qual as cargas de trabalho estão sendo executadas. Se o componente agregado estiver em contenção, isso significa que a alta utilização no agregado está afetando a latência de uma ou mais cargas de trabalho. Um agregado consiste em todos os HDDs ou uma mistura de HDDs e SSDs (um agregado Flash Pool) ou uma mistura de HDDs e uma camada de nuvem (um agregado FabricPool). Um “Agregado SSD” consiste em todos os SSDs (um agregado all-flash) ou uma mistura de SSDs e uma camada de nuvem (um 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 estão impactando a latência de uma ou mais cargas de trabalho.

- **Sincronizar SnapMirror**

Representa o componente de software no cluster envolvido na replicação de dados do usuário do volume primário para o volume secundário em um relacionamento síncrono do SnapMirror . Se o componente de sincronização SnapMirror estiver em contenção, isso significa que a atividade das operações síncronas do SnapMirror está impactando a latência de uma ou mais cargas de trabalho.

Página de detalhes de volume/saúde

Você pode usar a página Detalhes do volume/saúde para visualizar informações detalhadas sobre um volume selecionado, como capacidade, eficiência de armazenamento, configuração, proteção, anotação e eventos gerados. Você também pode visualizar informações sobre os objetos relacionados e alertas relacionados para esse volume.

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas para o volume selecionado:

- **Alternar para a visualização de desempenho**

Permite que você navegue até a página de detalhes de Volume/Desempenho.

- **Ações**

- Adicionar alerta

Permite adicionar um alerta ao volume selecionado.

- Editar Limites

Permite modificar as configurações de limite para o volume selecionado.

- Anotar

Permite que você anote o volume selecionado.

- Proteger

Permite que você crie relacionamentos SnapMirror ou SnapVault para o volume selecionado.

- Relação

Permite que você execute as seguintes operações de relacionamento de proteção:

- Editar

Inicia a caixa de diálogo Editar relacionamento, que permite alterar políticas, agendamentos e taxas máximas de transferência existentes do SnapMirror para um relacionamento de proteção existente.

- Abortar

Cancela transferências em andamento para um relacionamento selecionado. Opcionalmente, ele permite que você remova o ponto de verificação de reinicialização para transferências diferentes da transferência de linha de base. Não é possível remover o ponto de verificação de uma transferência de linha de base.

- Quietude

Desativa temporariamente as atualizações agendadas para um relacionamento selecionado. Transferências que já estão em andamento devem ser concluídas antes que o relacionamento seja encerrado.

- Quebrar

Quebra o relacionamento entre os volumes de origem e destino e altera o destino para um volume de leitura e gravação.

- Remover

Exclui permanentemente o relacionamento entre a origem e o destino selecionados. Os volumes não são destruídos e as cópias do Snapshot nos volumes não são removidas. Esta operação não pode ser desfeita.

- Retomar

Permite transferências agendadas para um relacionamento desativado. No próximo intervalo de transferência agendado, um ponto de verificação de reinicialização será usado, se houver um.

- Ressincronizar

Permite que você resincronize um relacionamento previamente rompido.

- Inicializar/Atualizar

Permite que você execute uma transferência de linha de base pela primeira vez em um novo relacionamento de proteção ou execute uma atualização manual se o relacionamento já estiver inicializado.

- Ressincronização reversa

Permite restabelecer um relacionamento de proteção interrompido anteriormente, invertendo a função da origem e do destino, tornando a origem uma cópia do destino original. O conteúdo da origem é substituído pelo conteúdo do destino, e quaisquer dados mais recentes que os dados da cópia comum do Snapshot são excluídos.

- Restaurar

Permite restaurar dados de um volume para outro. Para obter informações, consulte ["Restaurando dados usando a página de detalhes de Volume/Saúde"](#).



Os botões Restaurar e Operação de relacionamento não estão disponíveis para volumes que estão em relacionamentos de proteção síncronos.

- **Ver volumes**

Permite que você navegue até a visualização Saúde: Todos os volumes.

Aba de 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:

- Estouro de instantâneo

Exibe o espaço de dados consumido pelas cópias do 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 em risco no volume thin-provisionado é gerado e que o espaço no volume thin-provisionado está em risco devido a problemas de capacidade agregada. A capacidade inutilizável é exibida somente para volumes com provisionamento fino.

- Gráfico de dados

Exibe a capacidade total de dados e a capacidade de dados utilizada do volume.

Se o crescimento automático estiver habilitado, 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 real de dados do volume para as seguintes condições:
 - O crescimento automático está desativado.
 - O volume habilitado para crescimento automático atingiu o tamanho máximo.
 - O volume provisionado de forma espessa habilitado para crescimento automático não pode crescer mais.
- Capacidade de dados do volume após considerar o tamanho máximo do volume (para volumes com provisionamento fino e para volumes com provisionamento denso quando o agregado tem espaço para o volume atingir o tamanho máximo)
- Capacidade de dados do volume após considerar o próximo tamanho de crescimento automático possível (para volumes com provisionamento denso que têm um limite de porcentagem de crescimento automático)

- Gráfico de cópias instantâneas

Este gráfico é exibido somente quando a capacidade do Snapshot usada ou a reserva do Snapshot não é zero.

Ambos os gráficos exibem a capacidade pela qual a capacidade do Snapshot excede a reserva do Snapshot se a capacidade do Snapshot usada exceder a reserva do Snapshot.

- **Capacidade Lógica**

Exibe as características lógicas do espaço do volume. O espaço lógico indica o tamanho real dos dados que estão sendo armazenados no disco sem aplicar as economias do uso das tecnologias de eficiência de armazenamento ONTAP .

- Relatório 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 com provisionamento fino.

Quando definido como Ativado, o tamanho lógico usado do volume não pode ser maior que o tamanho do volume físico definido atualmente.

- **Crescimento automático**

Exibe se o volume aumenta automaticamente quando fica sem espaço.

- **Garantia de Espaço**

Exibe o controle de configuração de FlexVol volume quando um volume remove blocos livres de um agregado. Esses blocos estarão então disponíveis para gravações em arquivos no volume. A garantia de espaço pode ser definida como uma das seguintes:

- Nenhum

Nenhuma garantia de espaço está configurada para o volume.

- Arquivo

O tamanho total de arquivos gravados de forma esparsa (por exemplo, LUNs) é garantido.

- Volume

O tamanho total do volume é garantido.

- Parcial

O volume FlexCache reserva espaço com base em seu tamanho. Se o tamanho do volume FlexCache for 100 MB ou mais, a garantia de espaço mínimo será definida como 100 MB por padrão. Se o tamanho do volume FlexCache for menor que 100 MB, a garantia de espaço mínimo será definida para o tamanho do volume FlexCache. Se o tamanho do volume FlexCache aumentar posteriormente, a garantia de espaço mínimo não será incrementada.



A garantia de espaço é Parcial quando o volume é do tipo Data-Cache.

- **Detalhes (Físicos)**

Exibe 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 utilizada) 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 em risco de volume com provisionamento fino é gerado para volumes com provisionamento fino, a quantidade de espaço usada pelo volume (capacidade usada) e a quantidade de espaço que está disponível no volume, mas não pode ser usada (capacidade inutilizável) devido a problemas de capacidade agregada são exibidas.

- **Reserva Instantânea**

Exibe a quantidade de espaço usado pelas cópias do Snapshot (capacidade utilizada) e a quantidade de espaço disponível para cópias do Snapshot (capacidade livre) no volume. Esses valores também são exibidos como uma porcentagem da reserva total de instantâneos.

Quando o evento Espaço em risco de volume com provisionamento fino é gerado para volumes com provisionamento fino, a quantidade de espaço usada pelas cópias de instantâneo (capacidade usada) e a quantidade de espaço que está disponível no volume, mas não pode ser usada para fazer cópias de instantâneo (capacidade inutilizável) devido a problemas de capacidade agregada, são exibidas.

- **Limites de volume**

Exibe os seguintes limites de capacidade de volume:

- Limiar quase cheio

Especifica a porcentagem em que um volume está quase cheio.

- Limiar Completo

Especifica a porcentagem em que um volume está cheio.

- **Outros detalhes**

- Crescimento automático de tamanho máximo

Exibe o tamanho máximo até o qual o volume pode crescer automaticamente. O valor padrão é 120% do tamanho do volume na criação. Este campo é exibido somente quando o crescimento automático está habilitado para o volume.

- Capacidade comprometida da cota Qtree

Exibe o espaço reservado nas cotas.

- Capacidade supercomprometida da cota Qtree

Exibe a quantidade de espaço que pode ser usada antes que o sistema gere o evento Volume Qtree Quota Overcommitted.

- Reserva Fracionária

Controla o tamanho da reserva de substituição. Por padrão, a reserva fracionária é definida como 100, indicando que 100% do espaço necessário é reservado para que os objetos fiquem totalmente protegidos contra sobregravações. Se a reserva fracionária for inferior a 100%, o espaço reservado para todos os arquivos com espaço reservado naquele volume será reduzido à porcentagem de reserva fracionária.

- Taxa de crescimento diário instantâneo

Exibe a alteração (em porcentagem ou em KB, MB, GB e assim por diante) que ocorre a cada 24 horas nas cópias do Snapshot no volume selecionado.

- Dias de instantâneos completos

Exibe o número estimado de dias restantes antes que o espaço reservado para as cópias do Snapshot no volume atinja o limite especificado.

O campo Dias para Snapshot Completo exibe um valor Não Aplicável quando a taxa de crescimento das cópias de Snapshot no volume é zero ou negativa, ou quando não há dados suficientes para calcular a taxa de crescimento.

- Exclusão automática de instantâneo

Especifica se as cópias de instantâneo são excluídas automaticamente para liberar espaço quando uma gravação em um volume falha devido à falta de espaço no agregado.

- Cópias de instantâneos

Exibe informações sobre as cópias do Snapshot no volume.

O número de cópias do Snapshot no volume é exibido como um link. Clicar no link abre a caixa de diálogo Cópias de instantâneo em um volume, que exibe detalhes das cópias de instantâneo.

A contagem de cópias do Snapshot é atualizada aproximadamente a cada hora; no entanto, a lista de cópias do Snapshot é atualizada no momento em que você clica no ícone. Isso pode resultar em uma diferença entre a contagem de cópias do Snapshot exibida na topologia e o número de cópias do Snapshot listadas quando você clica no ícone.

• Movimento de volume

Exibe o status da operação de movimentação de volume atual ou da última que foi executada no volume e outros detalhes, como a fase atual da operação de movimentação de volume que está em andamento, o agregado de origem, o agregado de destino, a hora de início, a hora de término e a hora de término estimada.

Também exibe 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**.

Guia de configuração

A guia Configuração exibe detalhes sobre o volume selecionado, como a política de exportação, o tipo de RAID, a capacidade e os 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 Hierarquia

Exibe a política de camadas definida para o volume; se o volume estiver implantado em um agregado habilitado para FabricPool. A política pode ser Nenhuma, Somente instantâneo, Backup, Automática ou Todas.

- VM de armazenamento

Exibe o nome do SVM que contém o volume.

- Caminho de junção

Exibe o status do caminho, que pode ser ativo ou inativo. O caminho no SVM no qual o volume está montado também é exibido. Você pode clicar no link **Histórico** para visualizar as cinco alterações mais recentes no caminho da junção.

- Política de Exportação

Exibe o nome da política de exportação criada para o volume. Você pode clicar no link para visualizar detalhes sobre as políticas de exportação, protocolos de autenticação e acesso habilitado nos volumes que pertencem ao SVM.

- Estilo

Exibe o estilo do volume. O estilo do volume pode ser FlexVol ou FlexGroup.

- Tipo

Exibe o tipo do volume selecionado. O tipo de volume pode ser Leitura-gravação, Compartilhamento de carga, Proteção de dados, Cache de dados ou Temporário.

- Tipo RAID

Exibe o tipo de 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 dos FlexGroups podem estar em agregados de tipos diferentes.

- Tipo SnapLock

Exibe o tipo de SnapLock do agregado que contém o volume.

- Expiração do SnapLock

Exibe a data de expiração do volume SnapLock .

- **Capacidade**

- Provisionamento fino

Exibe se o provisionamento fino está configurado para o volume.

- Crescimento automático

Exibe se o volume flexível cresce automaticamente dentro de um agregado.

- Exclusão automática de instantâneo

Especifica se as cópias de instantâneo são excluídas automaticamente para liberar espaço quando uma gravação em um volume falha devido à falta de espaço no agregado.

- Cotas

Especifica se as cotas estão habilitadas para o volume.

- **Eficiência**

- Compressão

Especifica se a compactação está habilitada ou desabilitada.

- Desduplicação

Especifica se a desduplicação está habilitada ou desabilitada.

- Modo de desduplicação

Especifica se a operação de desduplicação habilitada em um volume é uma operação manual, agendada ou baseada em política. Se o modo estiver definido como Agendado, o agendamento da operação será exibido e, se o modo estiver definido como uma política, o nome da política será exibido.

- Tipo de desduplicação

Especifica o tipo de operação de desduplicação em execução no volume. Se o volume estiver em um relacionamento SnapVault, o tipo exibido será SnapVault. Para qualquer outro volume, o tipo é exibido como Regular.

- Política de Eficiência de Armazenamento

Especifica o nome da política de eficiência de armazenamento que foi atribuída por meio do Unified Manager a este volume. Esta política pode controlar as configurações de compactação e desduplicação.

- **Proteção**

- Cópias de instantâneos

Especifica se as cópias automáticas de Snapshot estão habilitadas ou desabilitadas.

Aba de proteção

A guia Proteção exibe detalhes de proteção sobre o volume selecionado, como informações de atraso, tipo de relacionamento e topologia do relacionamento.

- **Resumo**

Exibe 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 Política de cópia de Snapshot local e gerenciada será exibida. As propriedades exibidas para relacionamentos SnapMirror e SnapVault incluem o seguinte:

- Volume de origem

Exibe o nome da origem do volume selecionado se o volume selecionado for um destino.

- Status de atraso

Exibe o status de atraso de atualização ou transferência de um relacionamento de proteção. O status

pode ser Erro, Aviso ou Crítico.

O status de atraso não é aplicável para relacionamentos síncronos.

- Duração do atraso

Exibe o tempo em que os dados no espelho ficam atrasados em relação à origem.

- Última atualização bem-sucedida

Exibe a data e a hora da atualização de proteção bem-sucedida mais recente.

A última atualização bem-sucedida não é aplicável para relacionamentos síncronos.

- Membro do Serviço de Armazenamento

Exibe Sim ou Não para indicar se o volume pertence e é gerenciado por um serviço de armazenamento.

- Versão Replicação Flexível

Exibe Sim, Sim com opção de backup ou Nenhum. Sim indica que a replicação do SnapMirror é possível mesmo se os volumes de origem e destino estiverem executando versões diferentes do software ONTAP . Sim com opção de backup indica a implementação da proteção SnapMirror com a capacidade de manter várias versões de cópias de backup no destino. Nenhum indica que a Replicação Flexível de Versão não está habilitada.

- Capacidade de Relacionamento

Indica os recursos 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 de parceiro de proteção.

- Tipo de relacionamento

Exibe qualquer tipo de relacionamento, incluindo Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync e Sync.

- Estado de relacionamento

Exibe o estado do relacionamento SnapMirror ou SnapVault . O estado pode ser Não Inicializado, SnapMirrored ou Interrompido. Se um volume de origem for selecionado, o estado do relacionamento não será aplicável e não será exibido.

- Status de transferência

Exibe o status de transferência do relacionamento de proteção. O status da transferência pode ser um dos seguintes:

- Abortando

As transferências do SnapMirror estão habilitadas; no entanto, uma operação de aborto de transferência que pode incluir a remoção do ponto de verificação está em andamento.

- Verificando

O volume de destino está passando por uma verificação de diagnóstico e nenhuma transferência está em andamento.

- Finalizando

Transferências SnapMirror estão habilitadas. O volume está atualmente na fase de pós-transferência para transferências incrementais do SnapVault .

- Parado

As transferências estão habilitadas e nenhuma transferência está em andamento.

- Em sincronia

Os dados nos dois volumes no relacionamento síncrono são sincronizados.

- Fora de sincronia

Os dados no volume de destino não estão sincronizados com o volume de origem.

- Preparando

Transferências SnapMirror estão habilitadas. O volume está atualmente na fase de pré-transferência para transferências incrementais do SnapVault .

- Na fila

Transferências SnapMirror estão habilitadas. Nenhuma transferência está em andamento.

- Silenciou

As transferências do SnapMirror estão desativadas. Nenhuma transferência está em andamento.

- Quietude

Uma transferência do SnapMirror está em andamento. Transferências adicionais estão desabilitadas.

- Transferindo

As transferências do SnapMirror estão habilitadas e uma transferência está em andamento.

- Transição

A transferência assíncrona de dados do volume de origem para o volume de destino foi concluída e a transição para a operação síncrona foi iniciada.

- Esperando

Uma transferência do SnapMirror foi iniciada, mas algumas tarefas associadas estão aguardando para serem enfileiradas.

- Taxa máxima de transferência

Exibe a taxa máxima de transferência para o relacionamento. A taxa máxima de transferência pode ser um valor numérico em quilobytes por segundo (Kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) ou terabytes por segundo (Tbps). Se Nenhum Limite for exibido, a transferência de linha de base entre relacionamentos será ilimitada.

- Política do 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 cofre assíncrono padrão. StrictSync indica a política de proteção Síncrona Estrita padrão, e Sync indica a política Síncrona padrão. Você pode clicar no nome da política para visualizar detalhes associados a ela, incluindo as seguintes informações:

- Prioridade de transferência
- Ignorar configuração de tempo de acesso
- Limite de tentativas
- Comentários
- Etiquetas SnapMirror
- Configurações de retenção
- Cópias reais do Snapshot
- Preservar cópias do Snapshot
- Limite de aviso de retenção
- Cópias de instantâneo sem configurações de retenção Em um relacionamento SnapVault em cascata, onde a origem é um volume de proteção de dados (DP), somente a regra “sm_created” se aplica.

- Cronograma de atualização

Exibe a programação do SnapMirror atribuída ao relacionamento. Posicionar o cursor sobre o ícone de informações exibe os detalhes da programação.

- Política de Snapshot Local

Exibe a política de cópia de instantâneo para o volume. A política é Padrão, Nenhuma ou qualquer nome dado a uma política personalizada.

- Protegido por

Exibe o tipo de proteção usado para o volume selecionado. Por exemplo, se um volume for protegido por relacionamentos de volume do Consistency Group e do SnapMirror, este campo exibirá o SnapMirror e o Consistency Group. Este campo também fornece um link que redireciona você para a página Relacionamentos para visualizar o status unificado do relacionamento. O link é aplicável somente a relacionamentos constituintes.

- Grupo de Consistência

Para volumes protegidos por relacionamentos de sincronização ativos do SnapMirror, esta coluna exibe o Grupo de Consistência do volume.

- **Visualizações**

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 relacionamento de proteção. A direção dos relacionamentos na topologia é exibida da esquerda para a direita, com a origem de cada relacionamento à esquerda e o destino à direita.

Linhas duplas em negrito especificam um relacionamento de espelho assíncrono, uma única linha em negrito especifica um relacionamento de cofre assíncrono, linhas duplas simples especificam um relacionamento de cofre de espelho assíncrono e uma linha em negrito e uma linha sem negrito especificam um relacionamento síncrono. A tabela abaixo indica se o relacionamento síncrono é StrictSync ou Sync.

Clicar com o botão direito do mouse em um volume exibe um menu no qual você pode escolher proteger o volume ou restaurar dados nele. Clicar com o botão direito do mouse em um relacionamento exibe um menu no qual você pode escolher editar, abortar, desativar, interromper, remover ou retomar um relacionamento.

Os menus não serão exibidos nas seguintes instâncias:

- Se as configurações do RBAC não permitirem esta ação, por exemplo, se você tiver apenas privilégios de operador
- Se o volume estiver em um relacionamento de proteção síncrona
- Quando o ID do volume é desconhecido, por exemplo, quando você tem um relacionamento entre clusters e o cluster de destino ainda não foi descoberto. Clicar 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 faltando ou que ainda não foi descoberto. Isso também pode indicar que as informações de capacidade estão faltando. Posicionar o cursor sobre o ponto de interrogação exibe informações adicionais, incluindo sugestões de ações corretivas.

A topologia exibe informações sobre capacidade de volume, atraso, cópias de instantâneo 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, informações sobre o atraso do volume e a última transferência de dados bem-sucedida serão exibidas em uma tabela de relacionamento sob a topologia. Nesse caso, a linha destacada na tabela indica o volume selecionado e, na visualização da topologia, as linhas em negrito com um ponto azul indicam a relação entre o volume selecionado e seu volume de origem.

As visualizações de topologia incluem as seguintes informações:

- Capacidade

Exibe a quantidade total de capacidade usada pelo volume. Posicionar o cursor sobre um volume na topologia exibe as configurações atuais de limite de aviso e 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. Desmarcar a caixa de seleção **Capacidade** oculta todas as informações de capacidade de todos os volumes na topologia.

- Atraso

Exibe a duração do atraso e o status do atraso dos relacionamentos de proteção de entrada. Desmarcar a caixa de seleção **Lag** oculta todas as informações de atraso para todos os volumes na topologia. Quando a caixa de seleção **Lag** estiver esmaecida, as informações de atraso do volume selecionado serão exibidas na tabela de relacionamento abaixo da topologia, bem como as informações de atraso de todos os volumes relacionados.

- Instantâneo

Exibe o número de cópias de Snapshot disponíveis para um volume. Desmarcar a caixa de seleção **Snapshot** oculta todas as informações de cópia do Snapshot para todos os volumes na topologia.

Clicando em um ícone de cópia do Snapshot () exibe a lista de cópias do Snapshot para um volume. A contagem de cópias do Snapshot exibida ao lado do ícone é atualizada aproximadamente a cada hora; no entanto, a lista de cópias do Snapshot é atualizada no momento em que você clica no ícone. Isso pode resultar em uma diferença entre a contagem de cópias do Snapshot exibida na topologia e o número de cópias do Snapshot listadas quando você clica no ícone.

- Última transferência bem-sucedida

Exibe a quantidade, duração, hora e data da última transferência de dados bem-sucedida. Quando a caixa de seleção **Última transferência bem-sucedida** estiver esmaecida, as informações da última transferência bem-sucedida para o volume selecionado serão exibidas na tabela de relacionamento abaixo da topologia, bem como as informações da última transferência bem-sucedida para todos os volumes relacionados.

- **História**

Exibe em um gráfico o histórico dos relacionamentos de proteção de entrada do SnapMirror e do SnapVault para o volume selecionado. Há três gráficos de histórico disponíveis: duração do atraso do relacionamento de entrada, duração da transferência do relacionamento de entrada e tamanho da transferência do relacionamento de entrada. As informações do histórico são exibidas somente quando você seleciona um volume de destino. Se você selecionar um volume primário, os gráficos ficarão vazios e a mensagem Nenhum dado encontrado será exibida. Se os volumes forem protegidos por relacionamentos síncronos do Consistency Group e do SnapMirror, as informações sobre a duração da transferência do relacionamento e o tamanho da transferência do relacionamento não serão exibidas.

Você pode selecionar um tipo de gráfico na lista suspensa na parte superior do painel Histórico. Você também pode visualizar detalhes de um período de tempo específico selecionando 1 semana, 1 mês ou 1 ano. Os gráficos de histórico podem ajudar você a identificar tendências: por exemplo, se grandes quantidades de dados estiverem sendo transferidas no mesmo horário do dia ou da semana, ou se o limite de aviso de atraso ou erro de atraso estiver sendo violado consistentemente, você pode tomar as medidas adequadas. Além disso, você pode clicar no botão **Exportar** para criar um relatório no formato CSV para o gráfico que você está visualizando.

Os gráficos do histórico de proteção exibem as seguintes informações:

- **Duração do atraso no 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 do atraso atingida no período de duração mostrado no eixo x. A linha horizontal laranja no gráfico representa o limite de erro de atraso, e a linha horizontal amarela representa o limite de aviso de atraso. Posicionar o cursor sobre essas linhas exibe a configuração do limite. 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 atingida 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.



Este gráfico não está disponível para volumes que estão em relacionamentos de proteção síncronos.

• Tamanho do Relacionamento Transferido

Exibe bytes, kilobytes, megabytes e assim por diante, 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.



Este 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 no formato CSV para o gráfico que você está visualizando.

Os gráficos podem estar vazios e a mensagem Nenhum dado encontrado pode ser 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 visualizar detalhes de um período de tempo específico selecionando 1 semana, 1 mês ou 1 ano. Os gráficos de histórico podem ajudar você a identificar tendências. Por exemplo, se o uso do volume estiver constantemente ultrapassando o limite de Quase Cheio, você pode tomar as medidas adequadas.

Os gráficos de histórico exibem as seguintes informações:

• Capacidade de volume utilizada

Exibe a capacidade utilizada no volume e a tendência de como a capacidade do volume é usada com base no histórico de uso, como gráficos de linhas em bytes, kilobytes, megabytes e assim por diante, no eixo vertical (y). O período de tempo é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode visualizar os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda apropriada. Por exemplo, quando você clica na legenda Capacidade de Volume Utilizada, a linha do gráfico Capacidade de Volume Utilizada fica oculta.

• Capacidade de volume utilizada vs. total

Exibe a tendência de como a capacidade do volume é usada com base no histórico de uso, bem como a capacidade usada, a capacidade total e os detalhes da economia de espaço com a deduplicação e a compactação, como gráficos de linhas, em bytes, quilobytes, megabytes e assim por diante, no eixo vertical (y). O período de tempo é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode visualizar os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda apropriada. Por exemplo, quando você clica na legenda Tendência de Capacidade Utilizada, a linha do gráfico Tendência de Capacidade Utilizada fica oculta.

- **Capacidade de volume utilizada (%)**

Exibe a capacidade utilizada no volume e a tendência de como a capacidade do volume é utilizada com base no histórico de uso, como gráficos de linhas, em porcentagem, no eixo vertical (y). O período de tempo é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode visualizar os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda apropriada. Por exemplo, quando você clica na legenda Capacidade de Volume Utilizada, a linha do gráfico Capacidade de Volume Utilizada fica oculta.

- **Capacidade de instantâneo usada (%)**

Exibe a reserva do Snapshot e o limite de aviso do Snapshot como gráficos de linha, e a capacidade usada pelas cópias do Snapshot como um gráfico de área, em porcentagem, no eixo vertical (y). O estouro do Snapshot é representado com cores diferentes. O período de tempo é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode visualizar os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda apropriada. Por exemplo, quando você clica na legenda do Snapshot Reserve, a linha do gráfico do Snapshot Reserve fica oculta.

Lista de eventos

A lista de 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 registro de data e hora em que o evento foi gerado será exibido.

Painel de Anotações Relacionadas

O painel Anotações relacionadas permite que você visualize detalhes das anotações associadas ao volume selecionado. Os detalhes incluem o nome da anotação e os valores da anotação que são aplicados ao volume. Você também pode remover anotações manuais do painel Anotações Relacionadas.

Painel de dispositivos relacionados

O painel Dispositivos relacionados permite que você visualize e navegue até SVMs, agregados, qtrees, LUNs e cópias de instantâneos relacionados ao volume:

- **Máquina Virtual de Armazenamento**

Exibe a capacidade e o status de integridade do SVM que contém o volume selecionado.

- **Agregar**

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 status de integridade dos volumes também é exibido, com base no nível de gravidade mais alto. Por exemplo, se um agregado contiver dez volumes, cinco dos quais exibem o status Aviso e os cinco restantes exibem o status Crítico, então o status exibido será Crítico. Este componente não aparece para volumes FlexGroup .

- **Qárvores**

Exibe o número de qtrees que o volume selecionado contém e a capacidade de qtrees com cota que o volume selecionado contém. A capacidade das qtrees com cota é exibida em relação à capacidade de dados do volume. O status de saúde das 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.

- **Ações da NFS**

Exibe o número e o status dos compartilhamentos NFS associados ao volume.

- **Ações de PMEs**

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 status de integridade dos LUNs também é exibido, com base no nível de gravidade mais alto.

- **Cotas de Usuário e Grupo**

Exibe o número e o status das cotas de usuários e grupos 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 serão exibidos somente se o volume selecionado contiver volumes clonados.

- **Volume principal**

Exibe o nome e a capacidade do volume pai de um volume FlexClone selecionado. O volume pai será exibido somente se o volume selecionado for um volume FlexClone .

Painel de Grupos Relacionados

O painel Grupos relacionados permite que você visualize a lista de grupos associados ao volume selecionado.

Painel de alertas relacionados

O painel Alertas relacionados permite que você visualize 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 integridade da VM de armazenamento

Você pode usar a página Detalhes da VM de armazenamento/Integridade para visualizar 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 visualizar informações sobre os objetos relacionados e alertas relacionados à VM de armazenamento.



Você pode monitorar somente a VM de armazenamento de dados.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas para a VM de armazenamento selecionada:

- **Alternar para a visualização de desempenho**

Permite que você navegue até a página de detalhes da VM de armazenamento/desempenho.

- **Ações**

- Adicionar alerta

Permite adicionar um alerta à VM de armazenamento selecionada.

- Anotar

Permite que você anote a VM de armazenamento selecionada.

- **Ver VMs de armazenamento**

Permite que você navegue até a visualização Saúde: Todas as VMs de armazenamento.

Aba de saúde

A guia Saúde exibe informações detalhadas sobre disponibilidade de dados, capacidade de dados e problemas de proteção de vários objetos, como volumes, agregados, NAS LIFs, SAN LIFs, LUNs, protocolos, serviços, compartilhamentos NFS e compartilhamentos CIFS.

Você pode clicar no gráfico de um objeto para visualizar a lista filtrada de objetos. Por exemplo, você pode clicar no gráfico de capacidade de volume que exibe avisos para visualizar a lista de volumes que têm problemas de capacidade com gravidade de 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 nenhum problema relacionado 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 já afetaram a disponibilidade de dados na VM de armazenamento. Por exemplo, são exibidas informações sobre os NAS LIFs e SAN LIFs que estão inativos e volumes que estão offline.

Você também pode visualizar informações sobre os protocolos e serviços relacionados que estão em

execução no momento, além do número e 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 nenhum problema relacionado 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 já afetaram a capacidade de dados na VM de armazenamento. Por exemplo, são exibidas informações sobre agregados que provavelmente violarão os valores limite definidos.

- **Problemas de proteção**

Fornecer uma visão geral rápida da integridade relacionada à proteção da VM de armazenamento 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 nenhum problema relacionado à proteção. Você também pode visualizar o status do relacionamento DR da VM de armazenamento para a VM de armazenamento selecionada. Os eventos de relacionamento de DR da VM de armazenamento são exibidos aqui e clicar nos eventos leva você para a página de detalhes do evento. Quando houver volumes desprotegidos, clicar no link levará você à exibição Integridade: Todos os volumes, onde você poderá visualizar 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 visualização Relacionamento: Todos os relacionamentos, onde você pode visualizar uma lista filtrada de detalhes do relacionamento de proteção. As informações abaixo do gráfico fornecem detalhes sobre problemas de proteção que podem afetar ou já afetaram a proteção de dados na VM de armazenamento. Por exemplo, são exibidas informações sobre volumes que têm uma reserva de cópias do Snapshot quase cheia ou sobre problemas de atraso no relacionamento do SnapMirror .

Aba de 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 FlexVol volume ou volume 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 de armazenamento.

- Disponível Garantido

Exibe o espaço garantido disponível para dados que estão disponíveis para volumes na VM de armazenamento.

- Não garantido

Exibe o espaço disponível restante para dados alocados para volumes com provisionamento fino na

VM de armazenamento.

• Volumes com problemas de capacidade

A lista Volumes com problemas de capacidade exibe, em formato tabular, detalhes sobre os volumes que apresentam problemas de capacidade:

◦ Status

Indica que o volume tem um problema relacionado à capacidade de gravidade indicada.

Você pode mover o ponteiro sobre o status para visualizar 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 visualizar informações como o nome do evento, a hora e a data em que o evento foi disparado, o nome do administrador ao qual o evento foi atribuído e a causa do evento. Você pode usar o botão **Ver 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 de gravidades diferentes. Entretanto, apenas a gravidade mais alta é exibida. Por exemplo, se um volume tiver dois eventos com gravidades de Erro e Aviso, somente a gravidade do Erro será exibida.

◦ Volume

Exibe o nome do volume.

◦ Capacidade de dados usada

Exibe, como um gráfico, informações sobre o uso da capacidade do volume (em porcentagem).

◦ Dias para completar

Exibe o número estimado de dias restantes antes que o volume atinja a capacidade máxima.

◦ Thin Provisioned

Exibe 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 usados no FlexGroup.

Guia de configuração

A guia Configuração exibe detalhes de configuração sobre a VM de armazenamento selecionada, como seu cluster, volume raiz, o tipo de volumes que ela contém (volumes FlexVol), políticas e proteção criada na VM

de armazenamento:

- **Visão geral**

- Conjunto

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 da 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. Também indica se um protocolo está ativo (●), abaixo (●), ou não está configurado (●).

- **Interfaces de rede de dados**

- NAS

Exibe o número de interfaces NAS associadas à VM de armazenamento. Também indica se as interfaces estão ativas (●) ou para baixo (●).

- SAN

Exibe o número de interfaces SAN associadas à VM de armazenamento. Também indica se as interfaces estão ativas (●) ou para baixo (●).

- FC-NVMe

Exibe o número de interfaces FC-NVMe associadas à VM de armazenamento. Também indica se as interfaces estão ativas (●) ou para baixo (●).

- **Interfaces de Rede de Gerenciamento**

- Disponibilidade

Exibe o número de interfaces de gerenciamento associadas à VM de armazenamento. Também indica se as interfaces de gerenciamento estão ativas (●) ou para baixo (●).

- **Políticas**

- Instantâneos

Exibe o nome da política de Snapshot criada na VM de armazenamento.

- 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**

- VM de armazenamento DR

Exibe se a VM de armazenamento selecionada é protegida, de destino ou desprotegida e o nome do destino no qual a VM de armazenamento está protegida. Se a VM de armazenamento selecionada for de destino, os detalhes da VM de armazenamento de origem serão exibidos. Em 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 de contagem leva você para a grade de relacionamento da VM de armazenamento filtrada na VM de armazenamento de origem.

- Volumes Protegidos

Exibe o número de volumes protegidos na VM de armazenamento selecionada em relação ao total de volumes. Se você estiver visualizando uma VM de armazenamento de destino, o link numérico será para os volumes de destino da VM de armazenamento selecionada.

- Volumes desprotegidos

Exibe o número de volumes desprotegidos na VM de armazenamento selecionada.

- **Serviços**

- Tipo

Exibe o tipo de serviço configurado na VM de armazenamento. O tipo pode ser Sistema de Nomes de Domínio (DNS) ou Serviço de Informações de Rede (NIS).

- Estado

Exibe o estado do serviço, que pode ser Ativo (), Abaixo (), ou Não Configurado ().

- Nome de domínio

Exibe os nomes de domínio totalmente qualificados (FQDNs) do servidor DNS para os serviços DNS ou do servidor NIS para os serviços NIS. Quando o servidor NIS está habilitado, o FQDN ativo do servidor NIS é exibido. Quando o servidor NIS é desabilitado, a lista de todos os FQDNs é exibida.

- Endereço IP

Exibe os endereços IP do servidor DNS ou NIS. Quando o servidor NIS está habilitado, o endereço IP ativo do servidor NIS é exibido. Quando o servidor NIS está desabilitado, a lista de todos os endereços IP é exibida.

Guia 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 Up (), Abaixo (), ou Desconhecido (). O status operacional de uma interface é determinado pelo status de suas portas físicas.

- **Status Administrativo**

Exibe o status administrativo da interface, que pode ser Ativo (🟢), Abaixo (🔴), 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 status administrativo pode ser diferente do status operacional. Entretanto, se o status administrativo de uma interface for Inativo, o status operacional será Inativo por padrão.

- **Endereço IP / WWPN**

Exibe o endereço IP para 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.

- **Papel**

Exibe a função da interface. As funções podem ser Dados ou Gerenciamento.

- **Porto de origem**

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 poderá ser diferente da porta inicial.

- **Porta definida**

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 Próxima Disponível. A política de failover não é aplicável para interfaces FC e iSCSI.

- **Grupos de Roteamento**

Exibe o nome do grupo de roteamento. Você pode ver mais informações sobre as rotas e o gateway de destino clicando no nome do grupo de roteamento.

Grupos de roteamento não são suportados pelo 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 Qtrees

A aba 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 do qtree para um ou mais qtrees.

Use o botão **Exportar** para criar um arquivo de valores separados por vírgula (.csv) contendo os detalhes de todas as qtrees monitoradas. 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 seu data center. Alguns campos qtrees adicionais aparecem no arquivo CSV exportado.

- **Status**

Exibe o status atual do qtree. O status pode ser Crítico (❌), Erro (⚠️), Aviso (⚠️), ou Normal (✅).

Você pode mover o ponteiro sobre o ícone de status para visualizar mais informações sobre o evento ou eventos gerados para o qtree.

Se o status da qtree for determinado por um único evento, você poderá visualizar informações como o nome do evento, a hora e a data em que o evento foi disparado, o nome do administrador ao qual o evento foi atribuído e a causa do evento. Você pode usar **Ver 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 de gravidades diferentes. Entretanto, apenas a gravidade mais alta é exibida. Por exemplo, se uma qtree tiver dois eventos com gravidades de Erro e Aviso, somente a gravidade do Erro será exibida.

- **Qárvore**

Exibe o nome da qtree.

- **Conjunto**

Exibe o nome do cluster que contém a qtree. Aparece somente no arquivo CSV exportado.

- **Máquina Virtual de Armazenamento**

Exibe o nome da máquina virtual de armazenamento (SVM) que contém a qtree. Aparece somente no arquivo CSV exportado.

- **Volume**

Exibe o nome do volume que contém o qtree.

Você pode mover o ponteiro sobre o nome do volume para ver mais informações sobre ele.

- **Cota definida**

Indica se uma cota está habilitada ou desabilitada na qtree.

- **Tipo de cota**

Especifica se a cota é para um usuário, grupo de usuários ou uma qtree. Aparece somente no arquivo 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 está definida, a coluna fica vazia. Aparece somente no arquivo CSV exportado.

- **Disco usado %**

Exibe a porcentagem de espaço em disco utilizado. Se um limite rígido de disco for definido, esse valor será baseado no limite rígido do disco. Se a cota for definida sem um limite rígido de disco, 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, “Não aplicável” será exibido na página de grade e o campo ficará em branco nos dados de exportação CSV.

- **Limite de disco rígido**

Exibe a quantidade máxima de espaço em disco alocado para o qtree. O Unified Manager gera um evento crítico quando esse limite é atingido e nenhuma outra gravação em disco é permitida. O valor é exibido como “Ilimitado” para as seguintes condições: se a cota for definida sem um limite rígido de disco, se a cota não for definida ou se as cotas estiverem desativadas no volume ao qual a qtree pertence.

- **Limite de disco flexível**

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 flexível de disco, se a cota não for definida ou se as cotas estiverem desativadas no volume ao qual a qtree pertence. Por padrão, esta coluna está oculta.

- **Limite de disco**

Exibe o valor 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 disco, se a cota não for definida ou se as cotas estiverem desativadas no volume ao qual a qtree pertence. Por padrão, esta coluna está oculta.

- **Arquivos usados %**

Exibe a porcentagem de arquivos usados na qtree. Se o limite máximo do arquivo for definido, esse valor será baseado no limite máximo 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, “Não aplicável” será exibido na página de grade e o campo ficará em branco nos dados de exportação CSV.

- **Limite rígido de arquivo**

Exibe o limite rígido para o número de arquivos permitidos nas 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 ao qual a qtree pertence.

- **Limite flexível de arquivo**

Exibe o limite flexível para o número de arquivos permitidos nas qtrees. O valor é exibido como “Ilimitado” para as seguintes condições: se a cota for definida sem um limite flexível de arquivo, se a cota não for definida ou se as cotas estiverem desativadas no volume ao qual a qtree pertence. Por padrão, esta

coluna está oculta.

Guia Cotas de Usuário e Grupo

Exibe detalhes sobre as cotas de usuários e grupos de usuários para a VM de armazenamento selecionada. Você pode visualizar informações como o status da cota, o nome do usuário ou grupo de usuários, limites flexíveis e rígidos definidos nos discos e arquivos, quantidade de espaço em disco e número de arquivos usados, além do valor 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 vírgulas. 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 que você crie ou modifique 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 status pode ser Crítico (❌), Aviso (⚠️), ou Normal (✅).

Você pode mover o ponteiro sobre o ícone de status para visualizar mais informações sobre o evento ou eventos gerados para a cota.

Se o status da cota for determinado por um único evento, você poderá visualizar informações como o nome do evento, a hora e a data em que o evento foi disparado, o nome do administrador ao qual o evento foi atribuído e a causa do evento. Você pode usar **Ver 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 de gravidades diferentes. Entretanto, apenas a gravidade mais alta é exibida. Por exemplo, se uma cota tiver dois eventos com gravidades 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 vírgulas.

O valor é exibido como “Desconhecido” quando o ONTAP não fornece um nome de usuário válido devido

a 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 no qual a cota do usuário ou grupo de usuários está 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 utilizado. O valor é exibido como “Não aplicável” se a cota for definida sem um limite rígido de disco.

- **Limite de disco rígido**

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 outra gravação em disco é permitida. O valor é exibido como “Ilimitado” se a cota for definida sem um limite rígido de disco.

- **Limite de disco flexível**

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 flexível de disco. Por padrão, esta coluna está oculta.

- **Limite de disco**

Exibe o valor limite definido no espaço em disco. O valor é exibido como “Ilimitado” se a cota for definida sem um limite de disco. Por padrão, esta coluna está oculta.

- **Arquivos usados %**

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 de 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 flexível de arquivo**

Exibe o limite flexível para o número de arquivos permitidos na cota. O valor é exibido como “Ilimitado” se a cota for definida sem um limite flexível de arquivo. Por padrão, esta coluna está oculta.

- **Endereço de email**

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 de compartilhamentos NFS

A guia Compartilhamentos NFS exibe informações sobre compartilhamentos NFS, como seu status, o caminho associado ao volume (volumes FlexGroup ou FlexVol), níveis de acesso de 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**

Exibe o caminho no qual o volume está montado. Se uma política explícita de exportação do NFS for aplicada a uma qtree, a coluna exibirá o caminho do volume por meio do qual a qtree pode ser acessada.

- **Caminho de junção ativo**

Exibe se o caminho para acessar o 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, serão exibidos links para a qtree e o volume.

- **Estado do Volume**

Exibe o estado do volume que está sendo exportado. O estado pode ser Offline, Online, Restrito ou Misto.

- Off-line

Não é permitido acesso de leitura ou gravação ao volume.

- On-line

O acesso de leitura e gravação ao volume é permitido.

- Restrito

Operações limitadas, como reconstrução de paridade, são permitidas, mas o acesso a dados não é permitido.

- Misturado

Os constituintes de um volume FlexGroup não estão todos no mesmo estado.

- **Estilo de Segurança**

Exibe a permissão de acesso para os volumes que são exportados. O estilo de segurança pode ser UNIX, Unificado, NTFS ou Misto.

- UNIX (clientes NFS)

Arquivos e diretórios no volume têm permissões UNIX.

- Unificado

Arquivos e diretórios no volume têm um estilo de segurança unificado.

- NTFS (clientes CIFS)

Arquivos e diretórios no volume têm permissões NTFS do Windows.

- Misturado

Arquivos e diretórios no volume podem ter permissões UNIX ou Windows NTFS.

- **Permissão UNIX**

Exibe os bits de permissão do UNIX em um formato de string 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 ver detalhes sobre as regras associadas à política de exportação, como os protocolos de autenticação e a permissão de acesso.

Guia de compartilhamentos de PMEs

Exibe informações sobre os compartilhamentos SMB na VM de armazenamento selecionada. Você pode visualizar informações como o status do compartilhamento SMB, o nome do compartilhamento, o caminho associado à VM de armazenamento, o status do caminho de junção do compartilhamento, o objeto que o contém, o estado do volume que o contém, os dados de segurança do compartilhamento e as 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 Exibir mapeamento de usuário**

Inicia a caixa de diálogo Mapeamento de Usuário.

Você pode visualizar 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 visualizar detalhes do usuário e das permissões para o compartilhamento selecionado.

- **Status**

Exibe o status atual do compartilhamento. O status pode ser Normal (🟢) ou Erro (🔴).

- **Nome do compartilhamento**

Exibe o nome do compartilhamento SMB.

- **Caminho**

Exibe o caminho de junção no qual o compartilhamento é criado.

- **Caminho de junção ativo**

Exibe se o caminho para acessar o compartilhamento está ativo ou inativo.

- **Objeto Contendo**

Exibe o nome do objeto ao qual o compartilhamento pertence. O objeto contido pode ser um volume ou uma qtree.

Ao clicar no link, você pode ver detalhes sobre o objeto contido na respectiva página Detalhes. Se o objeto contido for uma qtree, serão exibidos links 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.

- Off-line

Não é permitido acesso de leitura ou gravação ao volume.

- On-line

O acesso de leitura e gravação ao volume é permitido.

- Restrito

Operações limitadas, como reconstrução de paridade, são permitidas, mas o acesso a dados não é permitido.

- Misturado

Os constituintes de um volume FlexGroup não estão todos no mesmo estado.

- **Segurança**

Exibe a permissão de acesso para os volumes que são exportados. O estilo de segurança pode ser UNIX, Unificado, NTFS ou Misto.

- UNIX (clientes NFS)

Arquivos e diretórios no volume têm permissões UNIX.

- Unificado

Arquivos e diretórios no volume têm um estilo de segurança unificado.

- NTFS (clientes CIFS)

Arquivos e diretórios no volume têm permissões NTFS do Windows.

- Misturado

Arquivos e diretórios no volume podem ter permissões UNIX ou 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 habilitado.

Você pode clicar no link para ver detalhes sobre as regras associadas à política de exportação, como protocolos de acesso e permissões. O link será desabilitado se a política de exportação estiver desabilitada para a VM de armazenamento selecionada.

- **Equivalente NFS**

Especifica se há um equivalente NFS para o compartilhamento.

Guia SAN

Exibe detalhes sobre LUNs, grupos de iniciadores e iniciadores para a VM de armazenamento selecionada. Por padrão, a visualização de LUNs é exibida. Você pode visualizar detalhes sobre os grupos iniciadores na guia Grupos de iniciadores e detalhes sobre os iniciadores na guia Iniciadores.

- **Guia LUNs**

Exibe detalhes sobre os LUNs que pertencem à VM de armazenamento selecionada. Você 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 operacional do host, a capacidade total de dados e o número de série do LUN. A coluna Desempenho do LUN fornece um link para a página de detalhes do LUN/Desempenho.

Você também pode visualizar informações sobre se o provisionamento fino está habilitado no LUN e se o LUN está mapeado para um grupo de iniciadores. Se estiver mapeado para um iniciador, você poderá visualizar os grupos de iniciadores e os iniciadores que estão mapeados para o LUN selecionado.

- **Guia Grupos de Iniciadores**

Exibe detalhes sobre grupos iniciadores. Você pode visualizar detalhes como o nome do grupo de iniciadores, o estado de acesso, o tipo de sistema operacional do host usado por todos os iniciadores no grupo e o protocolo suportado. Ao clicar no link na coluna de estado de acesso, você pode visualizar o estado de acesso atual do grupo iniciador.

- **Normal**

O grupo iniciador está conectado a vários caminhos de acesso.

- **Caminho Único**

O grupo iniciador está conectado a um único caminho de acesso.

- **Sem Caminhos**

Não há caminho de acesso conectado ao grupo iniciador.

Você pode ver se os grupos iniciadores são mapeados para todas as interfaces ou interfaces específicas por meio de um conjunto de portas. Quando você clica no link de contagem na coluna Interfaces mapeadas, todas as interfaces são exibidas ou interfaces específicas para um conjunto de

portas são exibidas. Interfaces mapeadas por meio do portal de destino não são exibidas. O número total de iniciadores e LUNs mapeados para um grupo de iniciadores é exibido.

Você também pode visualizar os LUNs e iniciadores mapeados para o grupo de iniciadores selecionado.

- **Guia de 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 de Anotações Relacionadas

O painel Anotações relacionadas permite que você visualize os detalhes das anotações associadas à VM de armazenamento selecionada. Os detalhes incluem o nome da anotação e os valores da anotação que são aplicados à VM de armazenamento. Você também pode remover anotações manuais do painel Anotações Relacionadas.

Painel de dispositivos relacionados

O painel Dispositivos relacionados permite que você visualize o cluster, os agregados e os volumes relacionados à VM de armazenamento:

- **Conjunto**

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 armazenamento selecionada. O status 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 Aviso e os cinco restantes exibem o status Crítico, o status exibido será Crítico.

- **Agregados Atribuídos**

Exibe o número de agregados atribuídos a uma VM de armazenamento. O status 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 status de integridade dos volumes também é exibido, com base no nível de gravidade mais alto. Quando há volumes FlexGroup na VM de armazenamento, a contagem também inclui FlexGroups; não inclui constituintes FlexGroup .

Painel de Grupos Relacionados

O painel Grupos relacionados permite que você visualize a lista de grupos associados à VM de armazenamento selecionada.

Painel de alertas relacionados

O painel Alertas relacionados permite que você visualize a lista de alertas criados para a VM de armazenamento 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 do cluster/saúde

A página Detalhes do cluster/integridade fornece informações detalhadas sobre um cluster selecionado, como integridade, capacidade e detalhes de configuração. Você também pode visualizar informações sobre as interfaces de rede (LIFs), nós, discos, dispositivos relacionados e alertas relacionados ao 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 que você execute as seguintes tarefas para o cluster selecionado:

- **Alternar para a visualização de desempenho**

Permite que você navegue até a página de detalhes do Cluster/Desempenho.

- **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, o que permite que o Unified Manager descubra alterações recentes no cluster.

Se o Unified Manager estiver pareado com o OnCommand Workflow Automation, a operação de redescoberta também readquirirá dados em cache do WFA, se houver.

Após o início da operação de redescoberta, um link para os detalhes do trabalho associado é exibido para permitir o rastreamento do status do trabalho.

- Anotar: permite que você anote o cluster selecionado.

- **Ver Clusters**

Permite que você navegue até a visualização Saúde: Todos os clusters.

Aba de saúde

Exibe informações detalhadas sobre a disponibilidade de dados e problemas de capacidade de dados de vários objetos de cluster, como nós, SVMs e agregados. Problemas de disponibilidade estão relacionados à capacidade de atendimento de dados dos objetos do cluster. Problemas de capacidade estão relacionados à capacidade de armazenamento de dados dos objetos do cluster.

Você pode clicar no gráfico de um objeto para visualizar uma lista filtrada dos objetos. Por exemplo, você pode clicar no gráfico de capacidade do SVM que exibe avisos para visualizar uma lista filtrada de SVMs. Esta lista contém SVMs que têm volumes ou qtrees com problemas de capacidade com um nível de gravidade de Aviso. Você também pode clicar no gráfico de disponibilidade de SVMs que exibe avisos para visualizar 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 nenhum problema relacionado 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 já afetaram a disponibilidade de dados no cluster. Por exemplo, são exibidas informações sobre prateleiras de disco que estão inativas e agregados que estão offline.



Os dados exibidos no gráfico de barras do SFO são baseados no estado HA dos nós. Os dados exibidos 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 com problemas de capacidade e objetos que não têm nenhum problema relacionado 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 impactar ou já impactaram a capacidade de dados no cluster. Por exemplo, são exibidas informações sobre agregados que provavelmente violarão os valores limite definidos.

Aba de 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 Usado

O tamanho real dos dados que estão sendo armazenados em todos os agregados neste cluster sem aplicar as economias do uso das tecnologias de eficiência de armazenamento ONTAP . Isso não inclui cópias do Snapshot.

- Redução de dados

Exibe a proporção sem cópias do Snapshot e com dois dígitos significativos, por exemplo, 1,8 para 1. Essa proporção é baseada nas configurações de eficiência de armazenamento do ONTAP .

- Usado

A capacidade física usada pelos dados em todos os agregados. Isso não inclui a capacidade usada para paridade, dimensionamento correto e reserva.

- Disponível

Exibe a capacidade disponível para dados.

- Peças de reposição

Exibe a capacidade de armazenamento disponível para todos os discos sobressalentes.

- Provisionado

Exibe a capacidade provisionada para todos os volumes subjacentes.

Detalhes

Exibe informações detalhadas sobre a capacidade utilizada e disponível. O cálculo exclui os dados agregados 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 dados.

- Provisionado

Exibe a capacidade provisionada para todos os volumes subjacentes.

- Peças de reposição

Exibe a capacidade de armazenamento disponível para 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 conectada para agregados habilitados para FabricPool no cluster. Um FabricPool pode ser licenciado ou não licenciado.

Divisão da capacidade física por tipo de disco

A área Divisão 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 ver mais informações sobre o tipo de disco na guia Discos.

- Capacidade Total Utilizável

Exibe a capacidade disponível e a capacidade extra dos discos de dados.

- HDD

Exibe graficamente a capacidade utilizada e a capacidade disponível de todos os discos de dados HDD no cluster. A linha pontilhada representa a capacidade extra dos discos de dados no HDD.

- Clarão

- Dados SSD

Exibe graficamente a capacidade utilizada e a capacidade disponível dos discos de dados SSD no cluster.

- Cache SSD

Exibe graficamente a capacidade de armazenamento dos discos de cache SSD no cluster.

- SSD sobressalente

Exibe graficamente a capacidade extra dos discos SSD, de dados e de cache no cluster.

- Discos não atribuídos

Exibe o número de discos não atribuídos no cluster.

Lista de agregados com problemas de capacidade

Exibe em formato tabular detalhes sobre a capacidade utilizada e a capacidade disponível dos agregados que apresentam problemas de risco de capacidade.

- Status

Indica que o agregado tem um problema relacionado à capacidade de certa gravidade.

Você pode mover o ponteiro sobre o status para visualizar mais informações sobre o evento ou eventos gerados para o agregado.

Se o status do agregado for determinado por um único evento, você poderá visualizar informações como o nome do evento, a hora e a data em que o evento foi disparado, o nome do administrador ao qual o evento foi atribuído e a causa do evento. Você pode clicar no botão **Ver 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 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 agregado pode ter vários eventos relacionados à capacidade de mesma gravidade ou de gravidades diferentes. Entretanto, apenas a gravidade mais alta é exibida. Por exemplo, se um agregado tiver dois eventos com níveis de gravidade Erro e Crítico, somente a gravidade Crítica será exibida.

- Agregar

Exibe o nome do agregado.

- Capacidade de dados usada

Exibe graficamente informações sobre o uso da capacidade agregada (em porcentagem).

- Dias para completar

Exibe o número estimado de dias restantes antes que o agregado atinja a capacidade máxima.

Guia de 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 status 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 OS

Exibe a versão do ONTAP que o cluster está executando. Se os nós no cluster estiverem executando versões diferentes do ONTAP, a versão mais antiga do ONTAP será exibida.

- Contato

Exibe detalhes sobre o administrador que você deve contatar em caso de problemas com o cluster.

- Localização

Exibe a localização do cluster.

- Personalidade

Identifica se este é um cluster configurado como All SAN Array.

Visão geral do cluster remoto

Fornece detalhes sobre o cluster remoto em uma configuração do MetroCluster . Essas informações são exibidas apenas para configurações do MetroCluster .

- Conjunto

Exibe o nome do cluster remoto. Você pode clicar no nome do cluster para navegar até a página de detalhes do cluster.

- Nome do host ou endereço IP

Exibe o FQDN, nome abreviado ou endereço IP do cluster remoto.

- Localização

Exibe a localização do cluster remoto.

Visão geral do MetroCluster

Fornecer detalhes sobre o cluster local em configurações MetroCluster sobre FC ou MetroCluster sobre IP. Essas informações são exibidas somente para configurações do MetroCluster sobre FC ou IP.

- Tipo

Exibe se o tipo do MetroCluster é de dois ou quatro nós. Para MetroCluster sobre IP, apenas quatro nós são suportados.

- Configuração

Exibe a configuração do MetroCluster sobre FC e IP, que pode ter os seguintes valores:

Para FC

- Configuração Stretch com cabos SAS
- Configuração Stretch com ponte FC-SAS
- Configuração de tecido com switches FC



Para um MetroCluster de quatro nós, somente a Configuração de Fabric com switches FC é suportada.

Para IP

- Configuração de IP com switches Ethernet (L2 ou L3, dependendo de como o cluster está configurado)
 - Comutação automatizada não planejada (AUSO)

Exibe se a alternância automatizada não planejada está habilitada para o cluster local. Por padrão, o AUSO é habilitado para todos os clusters em uma configuração MetroCluster de dois nós no Unified Manager. Você pode usar a interface de linha de comando para alterar a configuração AUSO. Isso é suportado apenas pelo MetroCluster via FC.

- Modo de comutação

Exibe o modo de comutação para a configuração do MetroCluster sobre IP. Os valores disponíveis são: `Active`, `Negotiated Switchover`, e `Automatic Unplanned Switchover`.

Nós

- Disponibilidade

Exibe o número de nós que estão ativos (●) ou para baixo (●) no cluster.

- Versões do sistema operacional

Exibe as versões do ONTAP que os nós estão executando, bem como o número de nós executando 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 ativos () ou para baixo () no cluster.

Interfaces de rede

- Disponibilidade

Exibe o número de LIFs não relacionados a dados que estão ativos () ou para baixo () no cluster.

- Interfaces de gerenciamento de cluster

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 do cluster.

- Interfaces Intercluster

Exibe o número de LIFs intercluster.

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

Exibido quando o cluster não oferece suporte a mediadores.

- Não configurado

Exibido quando o cluster suporta mediadores, mas o mediador não está configurado.

- Endereço IP

Exibe quando o cluster suporta mediadores e o mediador está configurado. O status do mediador é indicado pela cor. A cor verde indica que o status do mediador está acessível. A cor vermelha indica

que o status do mediador é inacessível.

Camadas de nuvem

Lista os nomes das camadas de nuvem às quais este 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 (Disponível ou Indisponível).

Guia de conectividade do MetroCluster

Exibe os problemas e o status de conectividade dos componentes do cluster na configuração do MetroCluster sobre FC. Um cluster é exibido em uma caixa vermelha quando o parceiro de recuperação de desastres do cluster tem problemas.



A guia Conectividade do MetroCluster é exibida somente para clusters que estão em uma configuração MetroCluster sobre FC.

Você pode navegar até 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 de contagem de um componente. Por exemplo, clicar no link de contagem do nó no cluster exibe a guia do nó na página de detalhes do cluster. Clicar no link de contagem de discos no cluster remoto exibe a guia de disco na página de detalhes do cluster remoto.



Ao gerenciar uma configuração MetroCluster de oito nós, clicar no link de contagem do componente Disk Shelves exibe apenas as prateleiras locais do par HA padrão. Além disso, não há como exibir as prateleiras locais no outro par de HA.

Você pode mover o ponteiro sobre os componentes para visualizar os detalhes e o status de conectividade dos clusters em caso de qualquer problema e para visualizar 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 visualizar informações como o nome do evento, a hora e a data em que o evento foi disparado, o nome do administrador ao qual 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 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.

Guia de replicação do MetroCluster

Exibe o status dos dados que estão sendo replicados em uma configuração MetroCluster sobre FC. Você pode usar a guia Replicação do MetroCluster para garantir a proteção de dados espelhando os dados de forma síncrona com os clusters já pareados. Um cluster é exibido em uma caixa vermelha quando o parceiro de recuperação de desastres do cluster tem 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 esta guia para verificar as conexões lógicas e o peering do

cluster local com o cluster remoto. Você pode visualizar 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 se refere ao cluster remoto.

Guia Interfaces de rede

Exibe detalhes sobre todos os LIFs não relacionados a dados criados no cluster selecionado.

Interface de rede

Exibe o nome do LIF criado no cluster selecionado.

Status operacional

Exibe o status operacional da interface, que pode ser Up (), Abaixo (), ou Desconhecido (). O status operacional de uma interface de rede é determinado pelo status de suas portas físicas.

Situação Administrativa

Exibe o status administrativo da interface, que pode ser Ativo (), Abaixo (), ou Desconhecido (). Você pode controlar o status administrativo de uma interface ao fazer alterações na configuração ou durante a manutenção. O status administrativo pode ser diferente do status operacional. Entretanto, se o status administrativo de um LIF for Inativo, o status operacional será Inativo por padrão.

Endereço IP

Exibe o endereço IP da interface.

Papel

Exibe a função da interface. As funções possíveis são LIFs de gerenciamento de cluster, LIFs de gerenciamento de nó, LIFs de cluster e LIFs intercluster.

Porto de origem

Exibe a porta física à qual a interface foi originalmente associada.

Porto atual

Exibe a porta física à qual a interface está atualmente associada. Após a migração do 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 ver mais informações sobre as rotas e o gateway de destino clicando no nome do grupo de roteamento.

Grupos de roteamento não são suportados pelo 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 os pares de HA, prateleiras de disco e portas:

Detalhes do HA

Fornecer uma representação pictórica do estado do HA e do status de integridade dos nós no par HA. O status de saúde do nó é indicado pelas seguintes cores:

- **Verde**

O nó está em condições de funcionamento.

- **Amarelo**

O nó assumiu o controle do nó parceiro ou o nó está enfrentando alguns problemas ambientais.

- **Vermelho**

O nó está inativo.

Você pode visualizar informações sobre a disponibilidade do par HA e tomar as medidas necessárias para evitar quaisquer riscos. Por exemplo, no caso de uma possível operação de aquisição, a seguinte mensagem é exibida: Possível failover de armazenamento.

Você pode visualizar uma lista de eventos relacionados ao par HA e seu ambiente, como ventiladores, fontes de alimentação, bateria NVRAM, cartões flash, processador de serviço e conectividade de prateleiras de disco. Você também pode visualizar o horário 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 visualizar detalhes sobre os nós.

Prateleiras de disco

Exibe informações sobre as prateleiras de disco no par HA.

Você também pode visualizar eventos gerados para as prateleiras de disco e os componentes ambientais, além do horário em que os eventos foram acionados.

- **ID da prateleira**

Exibe o 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 voltagem. Os detalhes

ambientais são exibidos como ícones nas seguintes cores:

- **Verde**

Os componentes ambientais estão funcionando corretamente.

- **Cinza**

Não há dados disponíveis para os componentes ambientais.

- **Vermelho**

Alguns componentes ambientais estão inativos.

- **Estado**

Exibe o estado da prateleira do disco. Os estados possíveis são Offline, Online, Sem status, Inicialização necessária, Ausente e Desconhecido.

- **Modelo**

Exibe o número do modelo da prateleira de disco.

- **Prateleira de Disco Local**

Indica se a prateleira de disco está localizada no cluster local ou no cluster remoto. Esta coluna é exibida somente para clusters em uma configuração MetroCluster .

- **ID único**

Exibe o identificador exclusivo da prateleira de disco.

- **Versão do firmware**

Exibe a versão do firmware da prateleira de disco.

Portos

Exibe informações sobre as portas FC, FCoE e Ethernet associadas. Você pode visualizar detalhes sobre as portas e os LIFs associados clicando nos ícones de porta.

Você também pode visualizar os eventos gerados para as portas.

Você pode visualizar 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.

- **Papel**

Exibe a função da porta. As funções possíveis são Cluster, Dados, Intercluster, Gerenciamento de Nós e Indefinido.

- **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.

- Revisão de firmware

Exibe a revisão do firmware da porta FC/FCoE.

- Status

Exibe o estado atual da porta. Os estados possíveis são Ativo, Inativo, Link Não Conectado ou Desconhecido (?).

Você pode visualizar os eventos relacionados ao porto na lista de Eventos. Você também pode visualizar os detalhes do LIF associado, como nome do LIF, status operacional, endereço IP ou WWPN, protocolos, nome do SVM associado ao LIF, porta atual, política de failover e grupo de failover.

Aba Discos

Exibe detalhes sobre os discos no cluster selecionado. Você pode visualizar informações relacionadas ao disco, como o número de discos usados, discos sobressalentes, discos quebrados e discos não atribuídos. Você também pode visualizar 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, 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 visualizar 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 de contagem do tipo de disco efetivo, os discos do estado selecionado e do tipo efetivo serão exibidos. Por exemplo, se você clicar no link de contagem para o estado do disco Quebrado e tipo efetivo SAS, todos os discos com o estado do disco Quebrado e tipo efetivo SAS 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, esta coluna é classificada para exibir os estados na seguinte ordem: Quebrado, Não atribuído, Sem suporte, Sobressalente, Agregado e Compartilhado.

Disco local

Exibe Sim ou Não para indicar se o disco está localizado no cluster local ou no cluster remoto. Esta coluna é exibida somente para clusters em uma configuração MetroCluster .

Posição

Exibe a posição do disco com base no seu tipo de contêiner: por exemplo, Cópia, Dados ou Paridade. Por padrão, esta coluna está oculta.

Agregados Impactados

Exibe o número de agregados afetados devido à falha do disco. Você pode mover o ponteiro sobre o link de contagem para visualizar os agregados impactados e, em seguida, clicar no nome do agregado para visualizar os detalhes do agregado. Você também pode clicar na contagem agregada para visualizar a lista de agregados impactados na exibição Saúde: Todos os agregados.

Nenhum valor é exibido nesta coluna para os seguintes casos:

- Para discos quebrados quando um cluster contendo tais discos é adicionado ao Unified Manager
- Quando não há discos com falha

Pool de armazenamento

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 visualizar detalhes do pool de armazenamento.

Capacidade de armazenamento

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, esta 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 fins de criação e adição de agregados e gerenciamento de sobressalentes. 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 fica em branco para discos que não sejam SSD.

Vida útil nominal usada em %

Exibe em porcentagem uma estimativa da vida útil do SSD, com base no uso real do SSD e na previsão do fabricante sobre a vida útil do SSD. Um valor maior que 99 indica que a resistência estimada foi consumida, mas pode não indicar falha do SSD. Se o valor for desconhecido, o disco será omitido.

Firmware

Exibe a versão do firmware do disco.

RPM

Exibe as revoluções por minuto (RPM) do disco. Por padrão, esta coluna está oculta.

Modelo

Exibe o número do modelo do disco. Por padrão, esta coluna está oculta.

Fornecedor

Exibe o nome do fornecedor do disco. Por padrão, esta coluna está oculta.

ID da prateleira

Exibe o ID da prateleira onde o disco está localizado.

Baía

Exibe o ID do compartimento onde o disco está localizado.

Painel de Anotações Relacionadas

Permite que você visualize 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. Você também pode remover anotações manuais do painel Anotações Relacionadas.

Painel de dispositivos relacionados

Permite que você visualize 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 de contagem para uma análise mais aprofundada daquele dispositivo específico.

Você pode usar o painel Parceiro do MetroCluster para obter contagem e também detalhes sobre o parceiro remoto do MetroCluster, juntamente com seus componentes de cluster associados, como nós, agregados e SVMs. O painel Parceiro do MetroCluster é exibido somente para clusters em uma configuração do MetroCluster.

O painel Dispositivos relacionados permite que você visualize e navegue até os nós, SVMs e agregados relacionados ao cluster:

Parceiro MetroCluster

Exibe o status de integridade do parceiro MetroCluster . Usando o link de contagem, você pode navegar mais 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 total utilizável sobre a 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 de Grupos Relacionados

Permite que você visualize a lista de grupos que inclui o cluster selecionado.

Painel de alertas relacionados

O painel Alertas relacionados permite que você visualize 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 de volumes" "Visualizando a lista de clusters e detalhes"](#)

Página de detalhes agregados/de saúde

Você pode usar a página Detalhes do agregado/saúde para visualizar informações detalhadas sobre o agregado selecionado, como capacidade, informações do disco, detalhes de configuração e eventos gerados. Você também pode visualizar 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 apenas para a capacidade local ou de nível de desempenho. A quantidade de espaço disponível na camada de nuvem não é refletida nos valores superafetados. Da mesma forma, os valores limite agregados são relevantes apenas para o nível de desempenho local.

Os botões de comando permitem que você execute as seguintes tarefas para o agregado selecionado:

- **Alternar para a visualização de desempenho**

Permite que você navegue até a página de detalhes Agregados/Desempenho.

- **Ações**

- Adicionar alerta

Permite adicionar um alerta ao agregado selecionado.

- Editar Limites

Permite modificar as configurações de limite para o agregado selecionado.

- **Ver Agregados**

Permite que você navegue até a visualização Saúde: Todos os agregados.

Aba de 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 limite usados pelo Unified Manager não são aplicáveis a agregados de raiz de nó. 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 limite são aplicados ao agregado raiz do nó.

- **Capacidade**

Exibe o gráfico de capacidade de dados e o gráfico de cópias de instantâneo, que exibem detalhes de capacidade sobre o agregado:

- Espaço Lógico Usado

O tamanho real dos dados que estão sendo armazenados no agregado sem aplicar as economias do uso das tecnologias de eficiência de armazenamento ONTAP .

- Usado

A capacidade física usada pelos dados no agregado.

- Comprometido demais

Quando o espaço no agregado está superlotado, o gráfico exibe um sinalizador com a quantidade superlotada.

- Aviso

Exibe uma linha pontilhada no local onde o limite de aviso é definido; 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; significa que o espaço no agregado está cheio. Se esse limite for violado, o evento Espaço Cheio será gerado.

- Gráfico de cópias instantâneas

Este gráfico é exibido somente quando a capacidade do Snapshot usada ou a reserva do Snapshot não é zero.

Ambos os gráficos exibem a capacidade pela qual a capacidade do Snapshot excede a reserva do Snapshot se a capacidade do Snapshot usada exceder a reserva do Snapshot.

- **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 a camada de nuvem é espelhada para outro provedor de nuvem (a “camada de espelho”), ambas as camadas de nuvem são exibidas aqui.

- **Detalhes**

Exibe informações detalhadas sobre capacidade.

- Capacidade total

Exibe a capacidade total no agregado.

- Capacidade de dados

Exibe a quantidade de espaço usado pelo agregado (capacidade utilizada) e a quantidade de espaço disponível no agregado (capacidade livre).

- Reserva Instantânea

Exibe a capacidade de Snapshot usada e livre do agregado.

- Capacidade supercomprometida

Exibe o comprometimento excessivo agregado. O comprometimento excessivo de agregados permite que você forneça mais armazenamento do que o realmente disponível em um determinado agregado, desde que nem todo esse armazenamento esteja sendo usado no momento. Quando o provisionamento fino está em uso, o tamanho total dos volumes no agregado pode exceder a capacidade total do agregado.



Se você tiver comprometido demais seu agregado, deverá monitorar cuidadosamente o espaço disponível 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 de espelho), ambas as camadas de nuvem são exibidas aqui

- Espaço total de cache

Exibe o espaço total das unidades de estado sólido (SSDs) ou unidades de alocação que são adicionadas a um agregado do Flash Pool. Se você tiver habilitado o Flash Pool para um agregado, mas não tiver adicionado nenhum SSD, o espaço de cache será exibido como 0 KB.



Este campo fica oculto se o Flash Pool estiver desabilitado para um agregado.

- Limiares agregados

Exibe os seguintes limites de capacidade agregada:

- Limiar quase cheio

Especifica a porcentagem em que um agregado está quase cheio.

- Limiar Completo

Especifica a porcentagem em que um agregado está cheio.

- Limite quase supercomprometido

Especifica a porcentagem na qual um agregado está quase supercomprometido.

- Limite de excesso de comprometimento

Especifica a porcentagem na qual 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 às 14h e 12 GB às 18h, a taxa de crescimento diária (GB) para esse agregado é de 2 GB.

- Movimento de volume

Exibe o número de operações de movimentação de volume que estão em andamento:

- Volumes 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, o agregado para o qual o volume foi movido, o status da operação de movimentação do volume e o horário 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 do qual o volume foi movido, o status da operação de movimentação do volume e o horário de término estimado.

- Capacidade estimada utilizada após movimentação de volume

Exibe a quantidade estimada de espaço usado (como uma porcentagem e em KB, MB, GB e assim por diante) no agregado após a conclusão das operações de movimentação de volume.

- **Visão geral da capacidade - Volumes**

Exibe gráficos que fornecem informações sobre a capacidade dos volumes contidos no agregado. A

quantidade de espaço usado pelo volume (capacidade utilizada) e a quantidade de espaço disponível (capacidade livre) no volume são exibidas. Quando o evento Espaço em risco de volume com provisionamento fino é gerado para volumes com provisionamento fino, a quantidade de espaço usada pelo volume (capacidade usada) e a quantidade de espaço que está disponível no volume, mas não pode ser usada (capacidade inutilizável) devido a problemas de capacidade agregada são exibidas.

Você pode selecionar o gráfico que deseja visualizar nas listas suspensas. Você pode classificar os dados exibidos no gráfico para exibir detalhes como tamanho usado, tamanho provisionado, capacidade disponível, taxa de crescimento diário mais rápida e 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 visualizar detalhes de volumes com provisionamento fino. 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 principais 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 visualizar mais informações, como o compartimento do disco, a prateleira e a velocidade de rotação, 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, detalhes gráficos dos discos compartilhados são exibidos. Quando os discos de dados contêm discos dedicados e discos compartilhados, 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 de 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 usados**

- **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 sobressalentes**

Exibe o tipo efetivo do disco, o número e a capacidade dos discos de dados sobressalentes que estão disponíveis para o nó no agregado selecionado.



Quando um agregado sofre failover para o nó parceiro, o Unified Manager não exibe todos os discos sobressalentes compatíveis com o agregado.

- **Cache SSD**

Fornecer detalhes sobre discos SSD de cache dedicado e discos SSD de cache compartilhado.

Os seguintes detalhes para os discos SSD de cache dedicado são exibidos:

- **Detalhes do RAID**

- Tipo

Exibe o tipo de 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 usados**

- 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 sobressalentes**

Exibe o tipo efetivo do disco, o número e a capacidade dos discos sobressalentes que estão disponíveis para o nó no agregado selecionado para cache.



Quando um agregado sofre failover para o nó parceiro, o Unified Manager não exibe todos os discos sobressalentes compatíveis com o agregado.

Fornece os seguintes detalhes para o cache compartilhado:

- **Pool de Armazenamento**

Exibe o nome do pool de armazenamento. Você pode mover o ponteiro sobre o nome do pool de armazenamento para visualizar os seguintes detalhes:

- **Status**

Exibe o status do pool de armazenamento, que pode ser íntegro ou não.

- **Alocações totais**

Exibe as unidades de alocação total e o tamanho no pool de armazenamento.

- **Tamanho da unidade de 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 íntegro.

- **Alocação Usada**

Exibe o número e o tamanho das unidades de alocação usadas pelos agregados. Você pode clicar no nome do agregado para visualizar 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 visualizar os detalhes agregados.

- **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 armazenamento

Exibe o número de pools de armazenamento.

- Tamanho total

Exibe o tamanho total dos pools de armazenamento.

- **Nível de Nuvem**

Exibe o nome da camada 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 provedor de nuvem (a camada de espelho), os detalhes de ambas as camadas de nuvem são exibidos aqui

Guia de configuração

A guia Configuração exibe detalhes sobre o agregado selecionado, como seu nó de cluster, tipo de bloco, tipo de RAID, tamanho do RAID e contagem de grupos de RAID:

- **Visão geral**

- Nó

Exibe o nome do nó que contém o agregado selecionado.

- Tipo de bloco

Exibe o formato do bloco do agregado: 32 bits ou 64 bits.

- Tipo RAID

Exibe o tipo de 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 SnapLock do agregado.

- **Nível de Nuvem**

Se este for um agregado habilitado para FabricPool, os detalhes da camada de nuvem serão exibidos. Alguns campos são diferentes dependendo do provedor de armazenamento. Quando a camada de nuvem é espelhada para outro provedor de nuvem (a “camada de espelho”), ambas as camadas de nuvem são exibidas aqui.

- Provedor

Exibe o nome do provedor de armazenamento, por exemplo, StorageGRID, Amazon S3, IBM Cloud

Object Storage, Microsoft Azure Cloud, Google Cloud Storage ou Alibaba Cloud Object Storage.

- Nome

Exibe o nome da camada de nuvem quando ela foi criada pelo ONTAP.

- Servidor

Exibe o FQDN da camada de nuvem.

- Porta

A porta usada para comunicação com o provedor de nuvem.

- Chave de acesso ou conta

Exibe a chave de acesso ou conta para a camada de nuvem.

- Nome do contêiner

Exibe o nome do bucket ou contêiner da camada de nuvem.

- SSL

Exibe se a criptografia SSL está habilitada para a camada 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 no 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 visualizar detalhes de um período de tempo específico selecionando 1 semana, 1 mês ou 1 ano. Os gráficos de histórico podem ajudar você a identificar tendências: por exemplo, se o uso agregado estiver constantemente ultrapassando o limite Quase Cheio, você pode tomar as medidas adequadas.

Os gráficos de histórico exibem as seguintes informações:

- **Capacidade agregada utilizada (%)**

Exibe a capacidade utilizada no agregado e a tendência de como a capacidade agregada é usada com base no histórico de uso como gráficos de linhas, em porcentagem, no eixo vertical (y). O período de tempo é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode visualizar os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda apropriada. Por exemplo, quando você clica na legenda Capacidade Utilizada, a linha do gráfico Capacidade Utilizada fica 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 linhas, em bytes, quilobytes, megabytes e assim por diante, no eixo vertical (y). O período de tempo é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode visualizar os detalhes de pontos específicos

no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda apropriada. Por exemplo, quando você clica na legenda Tendência de Capacidade Utilizada, a linha do gráfico Tendência de Capacidade Utilizada 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 linhas, como uma porcentagem, no eixo vertical (y). O período de tempo é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode visualizar os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma área específica. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda apropriada. Por exemplo, quando você clica na legenda Espaço Comprometido, a linha do gráfico Espaço Comprometido é ocultada.

Lista de eventos

A lista de 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 registro de data e hora de quando o evento foi gerado será exibido.

Painel de dispositivos relacionados

O painel Dispositivos relacionados permite que você visualize o nó do cluster, os volumes e os discos relacionados ao agregado:

- **Nó**

Exibe a capacidade e o status de integridade do nó que contém o agregado. Capacidade indica a capacidade total utilizável sobre a capacidade disponível.

- **Agregados no Nó**

Exibe o número e a capacidade de todos os agregados no nó do cluster que contém o agregado selecionado. O status 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 Aviso e os cinco restantes exibem o status Crítico, o status exibido será Crítico.

- **Volumes**

Exibe o número e a capacidade dos volumes FlexVol e FlexGroup no agregado; o número não inclui os constituintes do FlexGroup . O status de integridade dos volumes também é exibido, com base no nível de gravidade mais alto.

- **Pool de Recursos**

Exibe os pools de recursos relacionados ao agregado.

- **Discos**

Exibe o número de discos no agregado selecionado.

Painel de alertas relacionados

O painel Alertas relacionados permite que você visualize 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

["Visualizando detalhes do pool de armazenamento"](#)

Proteger e restaurar dados

Criar, monitorar e solucionar problemas de relacionamentos de proteção

O Unified Manager permite que você crie relacionamentos de proteção, monitore e solucione problemas de proteção de espelho e proteção de cofre de backup de dados armazenados em clusters gerenciados e restaure dados quando eles forem substituídos ou perdidos.

Tipos de proteção SnapMirror

Dependendo da implantação da sua topologia de armazenamento de dados, o Unified Manager permite que você configure vários tipos de relacionamentos de proteção do SnapMirror. Todas as variações da proteção SnapMirror oferecem proteção de recuperação de desastres contra failover, mas oferecem diferentes recursos em desempenho, flexibilidade de versão e proteção de múltiplas cópias de backup.

Relacionamentos de proteção assíncronos tradicionais do SnapMirror

A proteção assíncrona tradicional do SnapMirror fornece proteção de espelhamento de replicação de bloco entre volumes de origem e destino.

Em relacionamentos SnapMirror tradicionais, as operações de espelhamento são executadas mais rapidamente do que em relacionamentos SnapMirror alternativos porque a operação de espelhamento é baseada na replicação de bloco. No entanto, a proteção tradicional do SnapMirror exige que o volume de destino seja executado na mesma versão secundária ou posterior do software ONTAP que o volume de origem na mesma versão principal (por exemplo, versão 8.x para 8.x ou 9.x para 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 de versão

A proteção assíncrona do SnapMirror com replicação flexível de versão fornece proteção de espelhamento de replicação lógica entre volumes de origem e destino, mesmo se esses volumes estiverem sendo executados em versões diferentes do software ONTAP 8.3 ou posterior (por exemplo, versão 8.3 para 8.3.1, ou 8.3 para 9.1, ou 9.2.2 para 9.2).

Em relacionamentos SnapMirror com replicação flexível de versão, as operações de espelhamento não são executadas tão rapidamente quanto em relacionamentos SnapMirror tradicionais.

Devido à execução mais lenta, o SnapMirror com proteção de replicação flexível de versão não é adequado para implementação em nenhuma das seguintes circunstâncias:

- O objeto de origem contém mais de 10 milhões de arquivos a serem protegidos.
- 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 sejam mais de duas horas mais antigos que os dados na origem.)

Em qualquer uma das circunstâncias listadas, é necessária a execução mais rápida baseada em replicação

de bloco da proteção padrão do SnapMirror .

Proteção assíncrona SnapMirror com replicação flexível de versão e opção de backup

A proteção assíncrona SnapMirror com replicação flexível de versão e opção de backup fornece proteção de espelhamento entre volumes de origem e destino e a capacidade de armazenar várias cópias dos dados espelhados no destino.

O administrador de armazenamento pode especificar quais cópias do Snapshot são espelhadas da origem para o destino e também pode especificar por quanto tempo essas cópias serão mantidas no destino, mesmo que sejam excluídas na origem.

Em relacionamentos SnapMirror com replicação flexível de versão e opção de backup, as operações de espelhamento não são executadas tão rapidamente quanto em relacionamentos SnapMirror tradicionais.

SnapMirror Unified Replication (espelho e cofre)

A replicação unificada do SnapMirror permite que você configure a recuperação de desastres e o arquivamento no mesmo volume de destino. Assim como no SnapMirror, a proteção de dados unificada executa 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 instantânea do volume de origem e, em seguida, transfere essa cópia e os blocos de dados aos quais ela faz referência para o volume de destino. Assim como o SnapVault, a proteção de dados unificada não inclui cópias mais antigas do Snapshot na linha de base.

Proteção síncrona SnapMirror com sincronização estrita

A proteção síncrona do SnapMirror com sincronização "estrita" 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 para o volume primário será interrompida.

Proteção síncrona SnapMirror com sincronização regular

A proteção síncrona do SnapMirror com sincronização "regular" não exige que o volume primário e o secundário sejam sempre uma cópia verdadeira um 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 ficarão fora de sincronia e a E/S do cliente continuará no volume primário.



O botão Restaurar e os botões Operação de relacionamento não estão disponíveis ao monitorar relacionamentos de proteção síncronos na exibição Integridade: Todos os volumes ou na página Detalhes do volume/integridade.

Sincronização ativa do SnapMirror

O recurso de sincronização ativa do SnapMirror está disponível com o ONTAP 9.8 e versões posteriores, e você pode usá-lo para proteger aplicativos com LUNs, permitindo que os aplicativos façam failover de forma transparente, garantindo a continuidade dos negócios em caso de desastre.

Ele permite que você descubra e monitore os relacionamentos síncronos do SnapMirror para Grupos de Consistência (CGs) disponíveis em clusters e máquinas virtuais de armazenamento do Unified Manager. A sincronização ativa do SnapMirror é suportada em clusters AFF ou clusters All SAN Array (ASA), onde os clusters primário e secundário podem ser AFF ou ASA. A sincronização ativa do SnapMirror protege aplicativos com LUNs iSCSI ou FCP.

Ao visualizar os volumes e LUNs protegidos pelo relacionamento de sincronização ativa do SnapMirror , você pode obter uma visão unificada dos relacionamentos de proteção, grupos de consistência no inventário de volume, visualizar a topologia de proteção para relacionamentos de grupo de consistência e visualizar dados históricos para relacionamentos de grupo de consistência de até um ano. Você também pode baixar o relatório. Você também pode visualizar o resumo dos relacionamentos do Grupo de Consistência, pesquisar suporte para relacionamentos do 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 , consulte ["Documentação do ONTAP 9 para sincronização ativa do Snapmirror \(anteriormente SM-BC\)"](#) .

Configurar relacionamentos de proteção no Unified Manager

Há várias etapas que você deve executar para usar o Unified Manager e o OnCommand Workflow Automation para configurar relacionamentos do SnapMirror e do SnapVault para proteger seus dados.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter estabelecido relacionamentos de pares entre dois clusters ou duas máquinas virtuais de armazenamento (SVMs).
- O OnCommand Workflow Automation deve ser integrado ao Unified Manager:
 - ["Configurar a OnCommand Workflow Automation"](#).
 - ["Verificando o cache da fonte de dados do Unified Manager no Workflow Automation"](#).

Passos

1. Dependendo do tipo de relacionamento de proteção que você deseja criar, faça um dos seguintes:
 - ["Criar um relacionamento de proteção SnapMirror"](#).
 - ["Criar um relacionamento de proteção SnapVault"](#).
2. Se você quiser criar uma política para o relacionamento, dependendo do tipo de relacionamento que estiver criando, faça um dos seguintes procedimentos:
 - ["Criar uma política do SnapVault"](#).
 - ["Criar uma política do SnapMirror"](#).
3. ["Crie uma programação SnapMirror ou SnapVault"](#).

Configurar 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 “pacote WFA para gerenciar Clustered Data ONTAP” está incluído no WFA 5.1.1P6, portanto não há necessidade de baixar esse pacote do NetAppStorage Automation Store e instalá-lo separadamente no seu servidor WFA, como era necessário no passado. ["Pacote WFA para gerenciamento do ONTAP"](#)

- Você deve ter o nome do usuário do banco de dados criado no Unified Manager para dar suporte às conexões WFA e Unified Manager.

Este usuário do banco de dados deve ter recebido a função de usuário do Esquema de Integração.

- Você deve receber a função de Administrador ou a função de 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.
- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Automação de fluxo de trabalho**.
2. Na área **Usuário do banco de dados** da página **Automação de fluxo de trabalho**, selecione o nome e insira a senha do usuário do banco de dados que você criou para dar suporte às conexões do Unified Manager e da Automação de fluxo de trabalho.
3. Na área **Credenciais de automação de fluxo de trabalho** da página, insira o nome do host ou endereço IP (IPv4 ou IPv6), e o nome de usuário e a senha para a configuração de automação de fluxo de trabalho.

Você deve usar a porta do 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 Automação de fluxo de trabalho é exibida.

6. Clique em **Sim** para recarregar a interface da web e adicionar os recursos de automação de fluxo de trabalho.

Informações relacionadas

["Documentação da NetApp : OnCommand Workflow Automation \(versões atuais\)"](#)

Verificar o cache da fonte de dados do Unified Manager na Automação de Fluxo de Trabalho

Você pode determinar se o cache da fonte de dados do Unified Manager está funcionando corretamente verificando se a aquisição da fonte de dados foi bem-sucedida no Workflow Automation. Você pode fazer isso ao integrar o Workflow Automation ao Unified Manager para garantir que a funcionalidade do Workflow Automation esteja disponível após a integração.

Antes de começar

Você deve ter a função de Administrador ou a função de Arquiteto no Workflow Automation para executar esta tarefa.

Passos

1. Na interface do usuário de automação de fluxo de trabalho, 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 foi bem-sucedida e sem erros.

Os 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, você deve primeiro remover a conexão entre o OnCommand Workflow Automation e o Unified Manager e garantir que todos os trabalhos do OnCommand Workflow Automation em execução ou agendados sejam interrompidos.

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.

Remover a configuração do OnCommand Workflow Automation do Unified Manager

Você pode remover a configuração do OnCommand Workflow Automation do Unified Manager quando não quiser mais usar o Workflow Automation.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Automação de fluxo de trabalho** no menu Configuração à esquerda.
2. Na página **Automação de fluxo de trabalho**, clique em **Remover configuração**.

Executar failover e failback de relacionamento de proteção

Quando um volume de origem no seu relacionamento de proteção é desabilitado devido a uma falha de hardware ou um desastre, você pode usar os recursos de relacionamento de proteção no Unified Manager para tornar o destino de proteção acessível para leitura/gravação e fazer failover para esse volume até que a origem esteja online novamente; então, você pode fazer failback para a origem original quando ela estiver disponível para fornecer dados.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado o OnCommand Workflow Automation para executar esta operação.

Passos

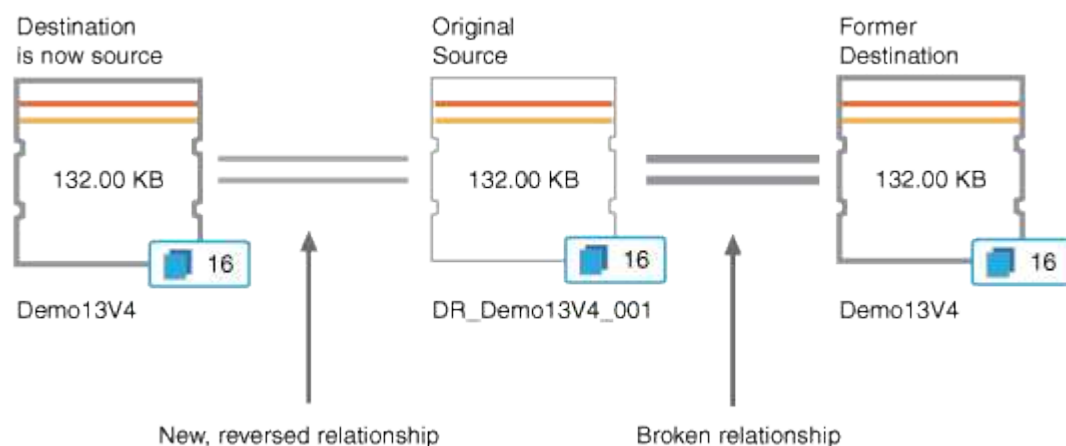
1. ["Quebre o relacionamento com o SnapMirror"](#).

Você deve interromper o relacionamento antes de poder converter o destino de um volume de proteção de dados para um volume de leitura/gravação e antes de poder reverter o relacionamento.

2. "Inverter a relação de proteção".

Quando o volume de origem original estiver disponível novamente, você poderá decidir restabelecer o relacionamento de proteção original restaurando o volume de origem. Antes de restaurar a origem, você deve sincronizá-la com os dados gravados no destino anterior. Use a operação de ressincronização reversa para criar um novo relacionamento de proteção invertendo as funções do relacionamento original e sincronizando o volume de origem com o destino anterior. Uma nova cópia de Snapshot de base é criada para o novo relacionamento.

O relacionamento inverso é semelhante a um relacionamento em cascata:



3. "Quebre o relacionamento invertido do SnapMirror".

Quando o volume de origem original for ressincronizado e puder servir dados novamente, use a operação break para quebrar o relacionamento invertido.

4. "Remover o relacionamento".

Quando o relacionamento invertido não for mais necessário, você deverá removê-lo antes de restabelecer o relacionamento original.

5. "Ressincronize o relacionamento".

Use a operação de ressincronização para sincronizar dados da origem para o destino e restabelecer o relacionamento original.

Interromper um relacionamento SnapMirror na página de detalhes Volume/Saúde

Você pode quebrar um relacionamento de proteção na página de detalhes do Volume/Integridade e interromper as transferências de dados entre um volume de origem e um volume de destino em um relacionamento SnapMirror. Você pode romper um relacionamento quando quiser migrar dados, para recuperação de desastres ou para testes de aplicativos. O volume de destino é alterado para um volume de leitura e gravação. Você não pode quebrar um relacionamento SnapVault.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, selecione na topologia o relacionamento SnapMirror que você deseja quebrar.
2. Clique com o botão direito do mouse no destino e selecione **Quebrar** no menu.

A caixa de diálogo Romper relacionamento é exibida.

3. Clique em **Continuar** para encerrar o relacionamento.
4. Na topologia, verifique se o relacionamento foi quebrado.

Relações de proteção reversa da página de detalhes de Volume/Saúde

Quando um desastre desabilita o volume de origem no seu relacionamento de proteção, você pode usar o volume de destino para fornecer dados convertendo-os para leitura/gravação enquanto repara ou substitui a origem. Quando a origem estiver novamente disponível para receber dados, você poderá usar a operação de resincronização reversa para estabelecer o relacionamento na direção reversa, sincronizando os dados na origem com os dados no destino de leitura/gravação.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.
- 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 quanto o destino devem estar online.
- A origem não deve ser o destino de outro volume de proteção de dados.
- Ao executar esta tarefa, os dados na origem que são mais recentes que os dados na cópia comum do Snapshot são excluídos.
- As políticas e programações criadas no relacionamento de resincronização reversa são as mesmas que aquelas no relacionamento de proteção original.

Se políticas e cronogramas não existirem, eles serão criados.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, localize na topologia o relacionamento SnapMirror no qual você deseja reverter a origem e o destino e clique com o botão direito do mouse.
2. Selecione **Ressincronização reversa** no menu.

A caixa de diálogo Ressincronização reversa é exibida.

3. Verifique se o relacionamento exibido na caixa de diálogo **Ressincronização reversa** é aquele para o qual você deseja executar a operação de resincronização reversa e clique em **Enviar**.

A caixa de diálogo Ressincronização reversa é fechada e um link de tarefa é exibido na parte superior da página de detalhes Volume/Saúde.

4. **Opcional:** Clique em **Exibir trabalhos** na página de detalhes **Volume / Saúde** para rastrear o status de cada trabalho de ressincronização reversa.

Uma lista filtrada de trabalhos é exibida.

5. **Opcional:** Clique na seta **Voltar** no seu navegador para retornar à página de detalhes **Volume / Saúde**.

A operação de ressincronização reversa é concluída quando todas as tarefas do trabalho são concluídas com sucesso.

Remover um relacionamento de proteção da página de detalhes de Volume/Saúde

Você pode remover um relacionamento de proteção para excluir permanentemente um relacionamento existente entre a origem e o destino selecionados: por exemplo, quando você deseja criar um relacionamento usando um destino diferente. Esta operação remove todos os metadados e não pode ser desfeita.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, selecione na topologia o relacionamento SnapMirror que você deseja remover.
2. Clique com o botão direito do mouse 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.

O relacionamento é removido da página de detalhes Volume/Saúde.

Ressincronizar relacionamentos de proteção na página de detalhes de Volume/Saúde

Você pode ressincronizar dados em um relacionamento SnapMirror ou SnapVault que foi quebrado e então o destino foi transformado em leitura/gravação para que os dados na origem correspondam aos dados no destino. Você também pode ressincronizar quando uma cópia comum necessária do Snapshot no volume de origem for excluída, causando falha nas atualizações do SnapMirror ou SnapVault .

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado o OnCommand Workflow Automation.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, localize na topologia o relacionamento de proteção que você deseja ressincronizar e clique com o botão direito do mouse.

2. Selecione **Ressincronizar** no menu.

Como alternativa, no menu **Ações**, selecione **Relacionamento > Ressincronizar** para ressincronizar o relacionamento cujos detalhes você está visualizando no momento.

A caixa de diálogo Ressincronizar é exibida.

3. Na aba **Opções de ressincronização**, selecione uma prioridade de transferência e a taxa máxima de transferência.
4. Clique em **Cópias de instantâneo de origem**; em seguida, na coluna **Cópia de instantâneo**, clique em **Padrão**.

A caixa de diálogo Selecionar cópia do instantâneo de origem é exibida.

5. Se você quiser especificar uma cópia de Snapshot existente em vez de transferir a cópia de Snapshot padrão, clique em **Cópia de Snapshot existente** e selecione uma cópia de Snapshot na lista.
6. Clique em **Enviar**.

Você retornará à caixa de diálogo Ressincronizar.

7. Se você selecionou mais de uma fonte para ressincronizar, clique em **Padrão** para a próxima fonte para a qual deseja especificar uma cópia de Snapshot existente.
8. Clique em **Enviar** para iniciar o trabalho de ressincronização.

O trabalho de ressincronização é iniciado, você retorna à página de detalhes de Volume/Saúde e um link de trabalhos é exibido na parte superior da página.

9. **Opcional:** Clique em **Exibir trabalhos** na página **Detalhes do volume/saúde** para rastrear o status de cada trabalho de ressincronização.

Uma lista filtrada de trabalhos é exibida.

10. **Opcional:** Clique na seta **Voltar** no seu navegador para retornar à página de detalhes **Volume / Saúde**.

O trabalho de ressincronização é concluído quando todas as tarefas são concluídas com sucesso.

Resolver uma falha de trabalho de proteção

Este 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 neste fluxo de trabalho exigem que você efetue login usando a função de Administrador, você deve estar familiarizado com as funções necessárias para usar várias funcionalidades.

Neste cenário, você acessa a página Painel para verificar se há algum problema com seus trabalhos de proteção. Na área Incidente de Proteção, você percebe que há um incidente de Trabalho Encerrado, mostrando um erro de Falha de Trabalho de Proteção em um volume. Você investiga esse 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 na tarefa de proteção.



O texto vinculado ao evento é escrito no formato `object_name:/object_name - Error Name`, como `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

A página Detalhes do evento para a tarefa de proteção com falha é exibida.

2. Revise a mensagem de erro no campo Causa da área **Resumo** para determinar o problema e avaliar possíveis ações corretivas.

Ver "[Identificar o problema e executar ações corretivas para um trabalho de proteção com falha](#)".

Identificar o problema e executar ações corretivas para um trabalho de proteção com falha

Você analisa a mensagem de erro de falha da tarefa no campo Causa na página Detalhes do evento e determina que a tarefa falhou devido a um erro de cópia do instantâneo. Em seguida, prossiga para a página de detalhes Volume/Saúde para coletar mais informações.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

A mensagem de erro fornecida no campo Causa na página Detalhes do evento contém o seguinte texto sobre a tarefa 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 backup ou espelhamento não foi concluído com sucesso.

O trabalho 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`.

- Falha no trabalho de cópia do Snapshot para `0426cluster2_src_vol2snap` no volume de origem `cluster2_src_svm:/cluster2_src_vol2`.

Neste cenário, você pode identificar a causa e possíveis ações corretivas da falha do trabalho. No entanto, para resolver a falha, é necessário acessar a interface da Web do System Manager ou os comandos da CLI do ONTAP.

Passos

1. Você analisa a mensagem de erro e determina que uma tarefa de cópia do Snapshot falhou no volume de origem, indicando que provavelmente há um problema com seu volume de origem.

Opcionalmente, você pode clicar no link **Detalhes do trabalho** no final da mensagem de erro, mas para os propósitos deste cenário, você escolhe não fazer isso.

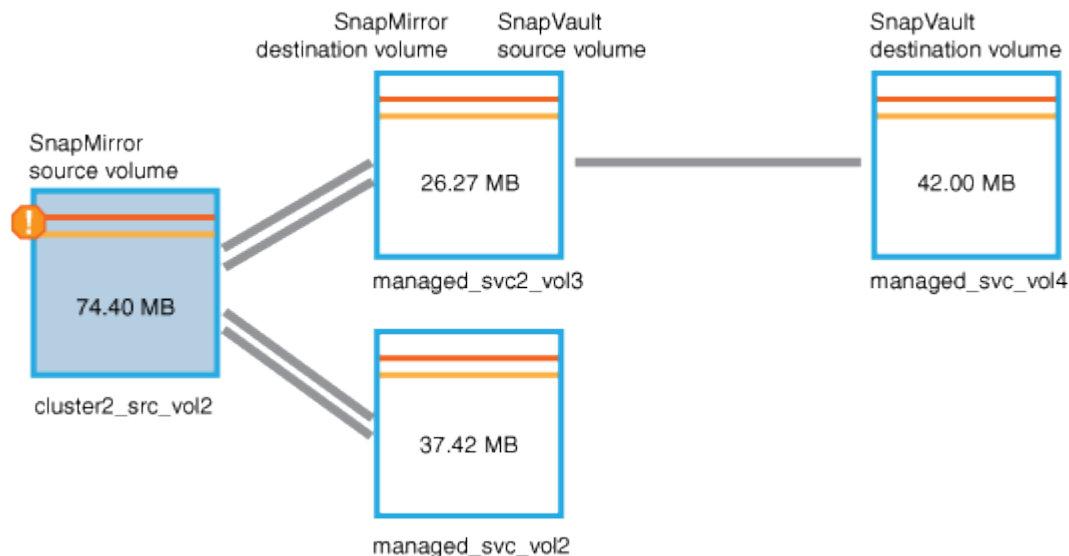
2. Você decide que quer tentar resolver o evento, então faz o seguinte:
 - a. Clique no botão **Atribuir a** e selecione **Eu** no menu.
 - b. Clique no botão **Reconhecer** para que você não continue recebendo notificações de alerta repetidas, caso alertas tenham sido definidos para o evento.
 - c. 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 **Origem** contém o nome do objeto de origem: neste caso, o volume no qual o trabalho de cópia do Snapshot foi agendado.

A página de detalhes do Volume/Saúde é exibida para `cluster2_src_vol2`, mostrando o conteúdo da aba **Proteção**.

4. Observando o gráfico de topologia de proteção, você vê um ícone de erro associado ao primeiro volume na topologia, que é o volume de origem do relacionamento SnapMirror .

Você também vê as barras horizontais no ícone do 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 veja que o volume excedeu o limite de erro, indicando um problema de capacidade.
6. Clique na aba **Capacidade**.

Informações de capacidade sobre volume `cluster2_src_vol2` exibe.

7. No painel **Capacidade**, você vê que há um ícone de erro no gráfico de barras, indicando novamente que a capacidade do volume ultrapassou o nível limite definido para o volume.
8. Abaixo do gráfico de capacidade, você vê que o crescimento automático de volume foi desabilitado e que uma garantia de espaço de volume foi definida.

Você pode decidir habilitar o crescimento automático, mas para os propósitos deste cenário, você decide investigar mais antes de tomar uma decisão sobre como resolver o problema de capacidade.

9. Você rola para baixo até a lista **Eventos** e vê que os eventos Falha na tarefa de proteção, Dias de volume até o limite máximo e Espaço de volume cheio foram gerados.
10. Na lista **Eventos**, clique no evento **Espaço de volume cheio** para obter mais informações, tendo decidido que esse evento parece mais relevante para seu problema de capacidade.

A página Detalhes do evento exibe o evento Espaço de volume cheio 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 vê Ações corretivas sugeridas.



As Ações Corretivas Sugeridas são exibidas apenas para alguns eventos, portanto você não vê essa área para todos os tipos de eventos.

Clique na lista de ações sugeridas que você pode executar para resolver o evento Espaço de Volume Cheio:

- Habilite o crescimento automático neste volume.
 - Redimensione o volume.
 - Habilite e execute a deduplicação neste volume.
 - Habilite e execute a compactação neste volume.
13. Você decide habilitar 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 **Dispositivos relacionados**.



Você pode clicar no nome do agregado para obter mais detalhes sobre ele.

Você determina que o agregado tem espaço suficiente para habilitar o crescimento automático de volume.

- b. No topo da página, observe o ícone que indica um incidente crítico e revise o texto abaixo do ícone.

Você determina que "Dias para atingir a plenitude: Menos de um dia | Taxa de crescimento diária: 5,4%".

14. Vá para o Gerenciador de Sistema ou acesse o ONTAP CLI para habilitar o `volume autogrow` opção.



Anote os nomes do volume e do agregado para que eles estejam disponíveis ao habilitar o crescimento automático.

15. Após resolver o problema de capacidade, retorne à página de detalhes do **Evento** do Unified Manager e marque o evento como resolvido.

Resolver problemas de atraso

Este fluxo de trabalho fornece um exemplo de como você pode resolver um problema de

atraso. Neste cenário, você é um administrador ou operador acessando a página Unified ManagerDashboard para verificar se há algum problema com seus relacionamentos de proteção e, se houver, encontrar soluções.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Na página Painel, você olha 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 no relacionamento do SnapMirror e clique nele.

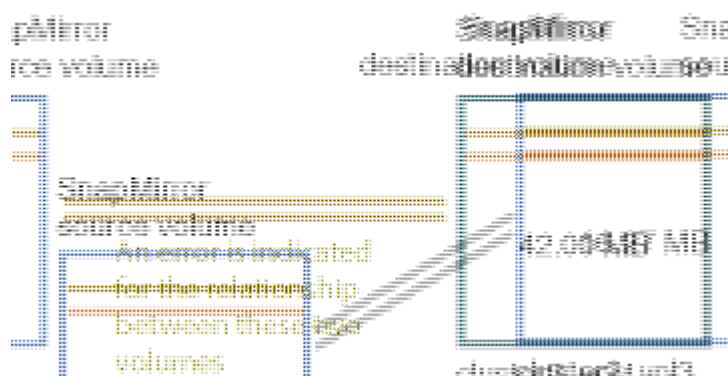
A página Detalhes do evento para o evento de erro de atraso é exibida.

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.
 - Reconheça ou resolva o evento.
3. Neste cenário, você clica no nome do objeto (neste caso, um volume) no campo Origem da área **Resumo** para obter detalhes sobre o volume.

A guia Proteção da página de detalhes Volume/Saúde é exibida.

4. Na aba **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 contornado em cinza escuro, e uma linha laranja dupla do volume de origem indica um erro de relacionamento do SnapMirror .



5. Clique em cada um dos volumes na cascata do SnapMirror .

Conforme você seleciona cada volume, as informações de proteção nas áreas Resumo, Topologia,

Histórico, Eventos, Dispositivos relacionados e Alertas relacionados mudam para exibir detalhes relevantes ao volume selecionado.

6. Você olha para a área **Resumo** e posiciona o cursor sobre o ícone de informações no campo **Atualizar cronograma** para cada volume.

Neste cenário, você observa que a política do SnapMirror é DPDefault, e a programação do SnapMirror é atualizada a cada hora, cinco minutos após a hora. Você percebe que todos os volumes no relacionamento estão tentando concluir uma transferência do SnapMirror ao mesmo tempo.

7. Para resolver o problema de atraso, modifique os agendamentos de dois dos volumes em cascata para que cada destino inicie uma transferência do SnapMirror depois que sua origem tiver concluído uma transferência.

Gerenciar e monitorar relacionamentos de proteção

O Active IQ Unified Manager permite que você crie relacionamentos de proteção, monitore e solucione problemas de relacionamentos SnapMirror e SnapVault em clusters gerenciados e restaure dados quando eles forem substituídos ou perdidos.

Para operações do SnapMirror, há dois tipos de replicação:

- Assíncrono

A replicação do volume primário para o secundário é determinada por um cronograma.

- 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 sentir algum impacto no desempenho ao executar entre 11 e 30 tarefas simultaneamente. Não é recomendado executar mais de 30 tarefas simultaneamente.

Exibir status de proteção de 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 **Painel**.
2. Dependendo se você deseja visualizar o status de proteção de dados de todos os clusters monitorados ou de 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 cluster ou todos os clusters no seu data center, esta página exibe o status de proteção de dados dos volumes protegidos por cópias de Snapshot ou políticas do SnapMirror e também exibe a contagem dos volumes desprotegidos.

Selecionar um cluster na lista **Cluster individual** exibe o status da proteção do Snapshot e do relacionamento do SnapMirror dos volumes protegidos naquele cluster.

Clicar nos eventos nesta página leva você para a página de detalhes do evento. Você pode clicar no link **Exibir tudo** para visualizar todos os eventos de proteção ativos na página de inventário do Gerenciamento de eventos. Você pode passar o mouse para visualizar as respectivas contagens e legendas. Você pode clicar:

- Os gráficos de barras para volumes desprotegidos e volumes protegidos por cópias de Snapshot permitem acessar a página Volumes e visualizar os detalhes.
- Os gráficos de barras de todos os relacionamentos vão para a página Relacionamentos, onde os detalhes são filtrados pelo cluster de origem.

Exibir status de proteção de volumes protegidos por cópias de Snapshot

Visão geral das cópias de instantâneo: Uma visão geral dos volumes protegidos por cópias de instantâneo, como:

- O número total de volumes protegidos e não protegidos por cópias de Snapshot.
- O número total de volumes que estão usando ou excedendo o espaço de reserva para as cópias do Snapshot.

Análise de cópias instantâneas detalha as seguintes informações:

- Eventos individuais para cópias do Snapshot, incluindo os eventos levantados nas últimas 24 horas.
- Gráfico detalhado para volumes protegidos e não protegidos por cópias de Snapshot.
- Volumes que usam, não usam e violam a capacidade de cópia reservada do Snapshot.
- Detalhamento das contagens de volume em termos do número de cópias do Snapshot.

Pontos a serem observados para cópias de instantâneos

- Para contar os volumes protegidos por cópias de Snapshot, são considerados os volumes de origem e de destino.
- O número de cópias do Snapshot retornadas é somente para os volumes que estão on-line e disponíveis.
- O intervalo do gráfico para o número de cópias do Snapshot é dinâmico. Ele é gerado com base no número de snapshots presentes no cluster selecionado.
- Para considerar um volume como protegido, o agendamento para a cópia de Snapshot do volume deve ser habilitado.
- O valor do espaço de reserva para cópias de Snapshot é importante para visualizar a quantidade de espaço em disco utilizado ou para calcular o espaço que pode ser recuperado se uma ou mais cópias de Snapshot forem excluídas.

Exibir status de proteção para relacionamentos SnapMirror

- Visão geral do SnapMirror *: Uma visão geral dos volumes protegidos pelas políticas do SnapMirror , como:
- O número de volumes protegidos pelas respectivas políticas do SnapMirror , como relacionamentos de volume do SnapMirror , recuperação de desastres de VM de armazenamento (SVM-DR) e suas combinações.
- O número total de relacionamentos do SnapMirror que apresentam atraso no objetivo do ponto de recuperação (RPO) com base no status do atraso.

- Análise SnapMirror * detalha as seguintes informações:
- Eventos individuais gerados para relacionamentos do SnapMirror , incluindo os eventos gerados 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 Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StricxtSync, grupo de consistência de sincronização ativa do SnapMirror e Sync.
- O número de relacionamentos saudáveis e não saudáveis.
- Quebra da contagem de relacionamento de volume. Você pode alternar os gráficos por tempo de atraso e status do RPO.
- Limites de atraso para relacionamentos não gerenciados. Você pode clicar no ícone de configurações

() para configurar as configurações de limite de atraso. Para mais informações, consulte ["Configurando configurações de limite de atraso para relacionamentos de proteção não gerenciados"](#).

Pontos a serem observados sobre relacionamentos SnapMirror

- Para contar relacionamentos do SnapMirror , os volumes de origem, que estão habilitados para leitura e gravação, são contados. Os volumes de destino e raiz não são considerados.
- Para o relacionamento SnapMirror , os eventos são exibidos para o cluster de origem.
- A contagem de relacionamentos do SnapMirror inclui o número de volumes com origens e destinos no mesmo cluster ou em clusters diferentes.
- A duração do atraso do RPO na replicação de dados é baseada na relação SnapMirror . O status é categorizado como `ok` , `warning` , ou `error` , com base no limite de relacionamento definido. Você pode verificar o status para determinar se os parâmetros estão funcionando conforme o esperado ou se é necessário resolver algum problema.
- Se um volume tiver vários relacionamentos SnapMirror , cada tipo de relacionamento será contado para o atraso do RPO.
- Os relacionamentos de volume são considerados prejudiciais se houver problemas na replicação de dados entre a origem e o destino, por exemplo, quando o relacionamento é interrompido.

Exibir clusters protegidos pela configuração do MetroCluster

O painel * Proteção do MetroCluster * na página * Proteção de Dados * exibe o número de clusters protegidos ou não protegidos pelo MetroCluster por meio da configuração 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 sua configuração do MetroCluster , consulte ["Monitoramento das configurações do MetroCluster"](#) .

Exibir relacionamentos de proteção de volume

Na exibição Relacionamento: Todos os relacionamentos e na página Relacionamentos de volume, você pode visualizar o status dos relacionamentos de volume existentes do SnapMirror e do SnapVault . 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 e assim por diante.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você também pode iniciar comandos de relacionamento a partir desta página.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Relacionamento > Todos os relacionamentos**.

A visualização Relacionamento: Todos os relacionamentos é exibida.

3. Escolha uma das seguintes maneiras de visualizar os detalhes da proteção de volume:
 - Para visualizar informações atuais sobre todos os relacionamentos de volume, permaneça na página padrão **Todos os relacionamentos**.
 - Para visualizar informações detalhadas sobre as tendências de transferência de volume ao longo de um período de tempo, no menu Exibir, selecione Relacionamento: Exibição de status de transferência do último mês.
 - Para visualizar informações detalhadas sobre a atividade de transferência de volume no dia a dia, no menu Exibir, selecione Relacionamento: Visualização da taxa de transferência do último mês.



As visualizações de transferência de volume exibem informações somente para volumes em relacionamentos assíncronos - volumes em relacionamentos síncronos não são mostrados.

Monitorar LUNs em um relacionamento 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 objetivo de tempo de recuperação zero (RTO) durante failover em ambientes SAN. Em uma implantação típica que oferece 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 entre os sites de origem e destino nesses LUNs compostos, garantindo transparência.

Para visualizar LUNs compostos, os clusters primário e secundário com os LUNs que fazem parte do relacionamento do Grupo de Consistência devem ser adicionados e descobertos no Unified Manager. Somente LUNs iSCSI e FCP são suportados.

Para obter informações sobre a sincronização ativa do SnapMirror, consulte "[Documentação do ONTAP 9 para sincronização ativa do SnapMirror \(anteriormente SM-BC\)](#)".

Para visualizar LUNs compostos em seu ambiente, siga estas etapas:

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > LUNs**.
2. No menu Exibir, selecione **Relacionamento > Todos os LUNs**.

A exibição Relacionamento: Todos os LUNs é exibida.

Você pode visualizar 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 parceiro. Você pode clicar em cada um desses componentes para obter uma visão detalhada. Clicar no Grupo de Consistência leva você para a página Relacionamentos.

Clicar no LUN do parceiro permite que você visualize os detalhes de configuração na guia SAN da página Detalhes da VM de armazenamento da VM de armazenamento na qual o LUN do parceiro está hospedado. Informações como iniciadores e grupos de iniciadores e outros aspectos do LUN parceiro são exibidas.

Você pode executar as funções padrão de nível de grade de classificação, filtragem, geração e upload de relatórios para os LUNs protegidos em seu ambiente.

Crie um relacionamento de proteção SnapVault na visualização Saúde: Todos os volumes

Você pode usar a exibição Integridade: Todos os volumes para criar relacionamentos do SnapVault para um ou mais volumes na mesma VM de armazenamento para habilitar backups de dados para fins de proteção.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

O menu **Proteger** não é exibido nas seguintes instâncias:

- Se as configurações do RBAC não permitirem esta ação: por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido: por exemplo, quando você tem um relacionamento entre clusters e o cluster de destino ainda não foi descoberto

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > 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 Integridade: 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 visualizar a guia * SnapVault* e configurar as informações do volume secundário.
5. Clique em **Avançado** para definir a deduplicação, a compactação, o crescimento automático e a garantia de espaço conforme necessário e, em seguida, clique em **Aplicar**.
6. Preencha a área **Informações de destino** e a área **Configurações de relacionamento** na aba * SnapVault*.
7. Clique em **Aplicar**.

Você retornará à visualização Saúde: Todos os volumes.

8. Clique no link do trabalho de configuração de proteção na parte superior da exibição **Saúde: Todos os volumes**.

Se você estiver criando apenas um relacionamento de proteção, a página Detalhes do trabalho será exibida; no entanto, se você estiver criando mais de um relacionamento de proteção, uma lista filtrada de todos os trabalhos associados à operação de proteção será exibida.

9. Faça um dos seguintes:

- Se você tiver apenas uma tarefa, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes das tarefas associadas à tarefa de configuração de proteção e para determinar quando a tarefa será concluída.
- Se você tem mais de um emprego:
 - i. Clique em um trabalho na lista de trabalhos.
 - ii. Clique em **Atualizar** para atualizar a lista de tarefas e os detalhes das tarefas associadas ao trabalho de configuração de proteção e para determinar quando o trabalho será concluído.
 - iii. Use o botão **Voltar** para retornar à lista filtrada e visualizar outro trabalho.

Crie um relacionamento de proteção SnapVault na página de detalhes Volume/Saúde

Você pode criar um relacionamento SnapVault usando a página de detalhes Volume/Saúde para que os backups de dados sejam habilitados para fins de proteção nos volumes.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho para executar esta tarefa.

O menu **Proteger** não é exibido nas seguintes instâncias:

- Se as configurações do RBAC não permitirem esta ação: por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido: por exemplo, quando você tem um relacionamento entre clusters e o cluster de destino ainda não foi descoberto

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Integridade**, clique com o botão direito do mouse em um volume na exibição de topologia que você deseja proteger.
2. Selecione **Proteger** > * SnapVault* no menu.

A caixa de diálogo Configurar proteção é iniciada.

3. Clique em * SnapVault* para visualizar a guia * SnapVault* e configurar as informações do recurso secundário.
4. Clique em **Avançado** para definir a deduplicação, a compactação, o crescimento automático e a garantia de espaço conforme necessário e, em seguida, 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**.

Você retornará à página de detalhes de Volume/Saúde.

7. Clique no link da tarefa de configuração de proteção na parte superior da página de detalhes **Volume / Saúde**.

A página Detalhes do trabalho é exibida.

8. Clique em **Atualizar** para atualizar a lista de tarefas e os detalhes das tarefas associadas ao trabalho de configuração de proteção e para determinar quando o trabalho será concluído.

Quando as tarefas do trabalho são concluídas, os novos relacionamentos são exibidos na exibição de topologia da página de detalhes de Volume/Integridade.

Crie um relacionamento de proteção SnapMirror na visualização Saúde: Todos os volumes

Usar a visualização Saúde: Todos os volumes permite que você crie vários relacionamentos de proteção do SnapMirror ao mesmo tempo selecionando mais de um volume na mesma VM de armazenamento.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

O menu **Proteger** não é exibido nas seguintes instâncias:

- Se as configurações do RBAC não permitirem esta ação: por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido: por exemplo, quando você tem um relacionamento entre clusters e o cluster de destino ainda não foi descoberto

Passos

1. Na visualização **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 Integridade: 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 aba * SnapMirror* e configurar as informações de destino.
3. Clique em **Avançado** para definir a garantia de espaço, conforme necessário, e depois clique em **Aplicar**.
4. Preencha a área **Informações de destino** e a área **Configurações de relacionamento** na aba * SnapMirror*.
5. Clique em **Aplicar**.

Você retornará à visualização Saúde: Todos os volumes.

6. Clique no link da tarefa de configuração de proteção na parte superior da visualização **Saúde: Todos os volumes**.

Se você estiver criando apenas um relacionamento de proteção, a página Detalhes do trabalho será exibida; no entanto, se você estiver criando mais de um relacionamento de proteção, uma lista de todos os trabalhos associados à operação de proteção será exibida.

7. Faça um dos seguintes:

- Se você tiver apenas uma tarefa, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes das tarefas associadas à tarefa de configuração de proteção e para determinar quando a tarefa será concluída.
- Se você tem mais de um emprego:
 - i. Clique em um trabalho na lista de trabalhos.
 - ii. Clique em **Atualizar** para atualizar a lista de tarefas e os detalhes das tarefas associadas ao trabalho de configuração de proteção e para determinar quando o trabalho será concluído.
 - iii. Use o botão **Voltar** para retornar à lista filtrada e visualizar outro trabalho.

Dependendo do SVM de destino especificado durante a configuração ou das opções habilitadas nas configurações avançadas, o relacionamento SnapMirror resultante pode ser uma das diversas variações possíveis:

- Se você especificou um SVM de destino que é executado na mesma versão ou em uma versão mais recente do ONTAP em comparação ao volume de origem, um relacionamento SnapMirror baseado em replicação de bloco é o resultado padrão.
- Se você especificou um SVM de destino que é executado na mesma versão 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 um relacionamento SnapMirror com 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 oferece suporte à replicação flexível de versão, um relacionamento SnapMirror com replicação flexível de versão é o resultado automático.

Crie um relacionamento de proteção SnapMirror na página de detalhes Volume/Saúde

Você pode usar a página de detalhes Volume/Saúde para criar um relacionamento SnapMirror para que a replicação de dados seja habilitada 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

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

O menu **Proteger** não é exibido nas seguintes instâncias:

- Se as configurações do RBAC não permitirem esta ação: por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido: por exemplo, quando você tem um relacionamento 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 sentir algum impacto no desempenho ao executar entre 11 e 30 tarefas simultaneamente. Não é recomendado executar mais de 30 tarefas simultaneamente.

Passos

1. Na **guia Proteção** da página de detalhes **Volume / Integridade**, clique com o botão direito do mouse na exibição de topologia no nome de um volume que você deseja proteger.
2. Selecione **Proteger** > * SnapMirror* no menu.

A caixa de diálogo Configurar proteção é exibida.

3. Clique em * SnapMirror* para visualizar a aba * SnapMirror* e configurar as informações de destino.
4. Clique em **Avançado** para definir a garantia de espaço, conforme necessário, e depois 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**.

Você retornará à página de detalhes de Volume/Saúde.

7. Clique no link da tarefa de configuração de proteção na parte superior da página de detalhes **Volume / Saúde**.

As tarefas e os detalhes do trabalho são exibidos na página Detalhes do trabalho.

8. Na página de detalhes do **Trabalho**, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes das tarefas associadas ao trabalho de configuração de proteção e para determinar quando o trabalho será concluído.
9. Quando as tarefas do trabalho estiverem concluídas, clique em **Voltar** no seu navegador para retornar à página de detalhes **Volume / Saúde**.

O novo relacionamento é exibido na exibição de topologia da página de detalhes Volume/Integridade.

Dependendo do SVM de destino especificado durante a configuração ou das opções habilitadas nas configurações avançadas, o relacionamento SnapMirror resultante pode ser uma das diversas variações possíveis:

- Se você especificou um SVM de destino que é executado na mesma versão ou em uma versão mais recente do ONTAP em comparação ao volume de origem, um relacionamento SnapMirror baseado em replicação de bloco é o resultado padrão.
- Se você especificou um SVM de destino que é executado na mesma versão 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 um relacionamento SnapMirror com replicação flexível de versão.
- Se você especificou um SVM de destino que é executado em uma versão anterior do ONTAP ou uma versão superior à do volume de origem e a versão anterior oferece suporte à replicação flexível de versão, um relacionamento SnapMirror com replicação flexível de versão é o resultado automático.

Crie um relacionamento SnapMirror com replicação flexível de versão

Você pode criar um relacionamento SnapMirror com replicação flexível de versão. A replicação flexível de versão permite que você implemente a proteção SnapMirror mesmo se os volumes de origem e destino forem executados em versões diferentes do ONTAP.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.
- Os SVMs de origem e destino devem ter uma licença SnapMirror habilitada.
- Os SVMs de origem e destino devem ser executados em uma versão do software ONTAP que suporte replicação flexível de versão.

O SnapMirror com replicação flexível de versão permite que você implemente a proteção SnapMirror mesmo em ambientes de armazenamento heterogêneos nos quais nem todo o armazenamento está sendo executado em uma versão do ONTAP; no entanto, as operações de espelhamento executadas no SnapMirror com replicação flexível de versão não são executadas tão rapidamente quanto seriam na replicação de bloco tradicional SnapMirror.

Passos

1. Exiba a caixa de diálogo **Configurar proteção** para o volume que você deseja proteger.
 - Se você estiver visualizando a guia Proteção da página de detalhes Volume/Saúde, clique com o botão direito do mouse na exibição de topologia que tem o nome de um volume que você deseja proteger e selecione **Proteger** > * SnapMirror* no menu.
 - Se você estiver visualizando a exibição Saúde: Todos os volumes, localize um volume que deseja proteger e clique com o botão direito nele; depois selecione **Proteger** > * SnapMirror* no menu. A caixa de diálogo Configurar proteção é exibida.

2. Clique em * SnapMirror* para visualizar a aba * 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 do ONTAP anterior ao volume de origem que você está protegendo, e se essa versão anterior oferecer suporte à 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 que o volume de origem, mas ainda quiser configurar o SnapMirror com replicação flexível de versão, clique em **Avançado** para habilitar a replicação flexível de versão e, em seguida, clique em **Aplicar**.
5. Clique em **Aplicar**.

Você retornará à página de detalhes de Volume/Saúde.

6. Clique no link da tarefa de configuração de proteção na parte superior da página de detalhes **Volume / Saúde**.

As tarefas e os detalhes do trabalho são exibidos na página Detalhes do trabalho.

7. Na página de detalhes do **Trabalho**, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes das tarefas associadas ao trabalho de configuração de proteção e para determinar quando o trabalho será

concluído.

- Quando as tarefas do trabalho estiverem concluídas, clique em **Voltar** no seu navegador para retornar à página de detalhes **Volume / Saúde**.

O novo relacionamento é exibido na exibição de topologia da página de detalhes Volume/Integridade.

Crie relacionamentos SnapMirror com replicação flexível de versão com opção de backup

Você pode criar um relacionamento SnapMirror com capacidade de replicação flexível de versão e opção de backup. O recurso de opção de backup permite que você implemente a proteção SnapMirror e também mantenha várias versões de cópias de backup no local de destino.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.
- Os SVMs de origem e destino devem ter uma licença SnapMirror habilitada.
- Os SVMs de origem e destino devem ter uma licença SnapVault habilitada.
- Os SVMs de origem e destino devem ser executados em uma versão do software ONTAP que suporte replicação flexível de versão.

Configurar o SnapMirror com capacidade de backup permite que você proteja seus dados com recursos de recuperação de desastres do SnapMirror, como capacidade de failover de volume, e ao mesmo tempo fornece recursos do SnapVault, como proteção de múltiplas cópias de backup.

Passos

1. Exiba a caixa de diálogo **Configurar proteção** para o volume que você deseja proteger.
 - Se você estiver visualizando a guia Proteção da página Detalhes do volume/saúde, clique com o botão direito do mouse na exibição de topologia no nome do volume que você deseja proteger e selecione **Proteger** > * SnapMirror* no menu.
 - Se você estiver visualizando a exibição Saúde: Todos os volumes, localize o volume que deseja proteger e clique com o botão direito nele; depois selecione **Proteger** > * SnapMirror* no menu. A caixa de diálogo Configurar proteção é exibida.
2. Clique em * SnapMirror* para visualizar a aba * 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 seleção **Version-Flexible Replication** ainda não estiver selecionada, marque-a agora.
6. Selecione a caixa de seleção **Com opção de backup** para habilitar a capacidade da opção de backup; depois clique em **Aplicar**.
7. Clique em **Aplicar**.

Você retornará à página de detalhes de Volume/Saúde.

8. Clique no link da tarefa de configuração de proteção na parte superior da página de detalhes **Volume / Saúde**.

As tarefas e os detalhes do trabalho são exibidos na página Detalhes do trabalho.

9. Na página de detalhes do **Trabalho**, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes das tarefas associadas ao trabalho de configuração de proteção e para determinar quando o trabalho será concluído.
10. Quando as tarefas do trabalho estiverem concluídas, clique em **Voltar** no seu navegador para retornar à página de detalhes **Volume / Saúde**.

O novo relacionamento é exibido na exibição de topologia da página de detalhes Volume/Integridade.

Configurar as definições de eficiência do destino

Você pode configurar as definições 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 do espaço em um volume de destino ou secundário.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Por padrão, as configurações de eficiência correspondem às do volume de origem, exceto as configurações de compactação em um relacionamento SnapVault, que são desabilitadas por padrão.

Passos

1. Clique na aba * SnapMirror* ou na aba * 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. Habilite ou desabilite as configurações de eficiência para deduplicação, compactação, crescimento automático e garantia de espaço, conforme necessário.
4. Clique em **Aplicar** para salvar suas seleções e retornar à caixa de diálogo **Configurar proteção**.

Crie agendamentos SnapMirror e SnapVault

Você pode criar agendamentos básicos ou avançados do SnapMirror e do SnapVault para habilitar transferências automáticas de proteção de dados em um volume de origem ou primário para que as transferências ocorram com mais ou menos frequência, dependendo da frequência com que os dados são alterados em seus volumes.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você já deve ter preenchido a área Informações de destino na caixa de diálogo Configurar proteção.
- Você deve ter configurado a Automação de Fluxo de Trabalho para executar esta tarefa.

Passos

1. Na guia * SnapMirror* ou * 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 você deseja dar à programação.
3. Selecione uma das seguintes opções:

- **Básico**

Selecione se você deseja criar uma programação básica no estilo intervalo.

- **Avançado**

Selecione se você deseja criar uma programação no estilo cron.

4. Clique em **Criar**.

O novo agendamento é exibido na lista suspensa Agendamento do SnapMirror ou Agendamento do SnapVault .

Crie relacionamentos em cascata ou em fanout para estender a proteção de um relacionamento de proteção existente

Você pode estender a proteção de um relacionamento existente criando um fanout a partir do volume de origem ou uma cascata a partir do volume de destino de um relacionamento existente. Você pode fazer isso quando precisar copiar dados de um site para vários sites ou para fornecer proteção adicional criando mais backups.

Você pode estender a proteção aos volumes usando o grupo de consistência, que é um contêiner que contém vários volumes para que você possa gerenciar todos eles como uma única entidade. Você pode visualizar o grupo de consistência de sincronização ativa do SnapMirror e o relacionamento do grupo de consistência síncrona na página Relacionamentos do Unified Manager.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

Passos

1. Clique em **Proteção > Relacionamentos**. Como alternativa, você pode visualizar os relacionamentos na página Detalhes do volume.
2. Na página **Relacionamentos de Volume**, selecione o relacionamento do SnapMirror do qual você deseja estender a proteção.
3. Na barra de ação, clique em **Estender proteção**.
4. No menu, selecione **Da Origem** ou **Do Destino**, dependendo se você está criando um relacionamento de fanout a partir da origem ou um relacionamento em cascata a partir do destino.
5. Selecione **Com SnapMirror** ou **Com SnapVault** dependendo do tipo de relacionamento de proteção que você está criando.

A caixa de diálogo **Configurar proteção** é exibida.



Isso pode ser feito na página de detalhes de relacionamento unificado/Relacionamento de volume e Volume/Saúde.

6. Preencha as informações conforme indicado na caixa de diálogo **Configurar proteção**.

Editar relacionamentos de proteção na página Relacionamentos de Volume

Você pode editar relacionamentos de proteção existentes para alterar a taxa máxima de transferência, a política de proteção ou o cronograma de proteção. Você pode editar um relacionamento para diminuir a largura de banda usada para transferências ou para aumentar a frequência de transferências agendadas, pois os dados mudam com frequência.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Os volumes selecionados devem ser destinos de relacionamento de proteção. Não é possível editar relacionamentos quando volumes de origem, volumes de compartilhamento de carga ou volumes que não são o destino de um relacionamento SnapMirror ou SnapVault são selecionados.

Passos

1. Na página **Relacionamentos de Volume**, selecione na lista de volumes um ou mais volumes no mesmo SVM para os quais você deseja editar as configurações de relacionamento e, em seguida, 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 aos relacionamentos selecionados.

Editar relacionamentos de proteção na página de detalhes de Volume/Saúde

Você pode editar relacionamentos de proteção existentes para alterar a taxa máxima de transferência 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 para aumentar a frequência de transferências agendadas, pois os dados mudam com frequência.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter instalado e configurado o Workflow Automation.

Os volumes selecionados devem ser destinos de relacionamento de proteção. Não é possível editar relacionamentos quando volumes de origem, volumes de compartilhamento de carga ou volumes que não são o destino de um relacionamento SnapMirror ou SnapVault são selecionados.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, localize na topologia o relacionamento de proteção que você deseja editar e clique com o botão direito do mouse.
2. Selecione **Editar** no menu.

Como alternativa, no menu **Ações**, selecione **Relacionamento > Editar** para editar o relacionamento cujos detalhes você está visualizando 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 aos relacionamentos selecionados.

Crie uma política SnapMirror para maximizar a eficiência de transferência

Você pode criar uma política do SnapMirror para especificar a prioridade de transferência do SnapMirror para relacionamentos de proteção. As políticas do SnapMirror permitem maximizar a eficiência da transferência da origem para o destino atribuindo prioridades para que transferências de prioridade mais baixa sejam programadas para serem executadas após transferências de prioridade normal.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.
- Esta tarefa pressupõe que você já tenha preenchido 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 do SnapMirror é exibida.

2. No campo **Nome da política**, digite o nome que você deseja dar 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 do SnapMirror .

Crie uma política do SnapVault para maximizar a eficiência da transferência

Você pode criar uma nova política do SnapVault para definir a prioridade de uma transferência do SnapVault . Você usa políticas para maximizar a eficiência das

transferências do primário para o secundário em um relacionamento de proteção.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.
- Você já deve ter preenchido 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**.

A guia SnapVault é exibida.

2. No campo **Nome da política**, digite o nome que você deseja dar à política.
3. No campo **Prioridade de transferência**, selecione a prioridade de transferência que você deseja atribuir à política.
4. **Opcional:** No campo **Comentário**, insira um comentário para a política.
5. Na área **Rótulo 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 na página Relacionamentos de Volume

Você pode abortar uma transferência de proteção de dados ativa quando quiser interromper uma replicação do SnapMirror que esteja em andamento. Você também pode limpar o ponto de verificação de reinicialização para transferências subsequentes à transferência de linha de base. Você pode abortar uma transferência quando ela entra 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

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

A ação de aborto não é exibida nas seguintes instâncias:

- Se as configurações do RBAC não permitirem esta ação: por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido: por exemplo, quando você tem um relacionamento entre clusters e o cluster de destino ainda não foi descoberto

Não é possível limpar o ponto de verificação de reinicialização para uma transferência de linha de base.

Passos

1. Para abortar 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 **Abortar**.

A caixa de diálogo Abortar transferência é exibida.

2. Se você quiser limpar o ponto de verificação de reinicialização 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 Abortar transferência é fechada, e o status do trabalho de aborto é exibido na parte superior da página Relacionamentos de volume, junto com um link para os detalhes do trabalho.

4. **Opcional:** Clique no link **Exibir detalhes** para ir para a página de detalhes do **Trabalho** para obter detalhes adicionais e visualizar o andamento do trabalho.

Abortar uma transferência ativa de proteção de dados na página de detalhes de Volume/Saúde

Você pode abortar uma transferência de proteção de dados ativa quando quiser interromper uma replicação do SnapMirror que esteja em andamento. Você também pode limpar o ponto de verificação de reinicialização de uma transferência se ela não for uma transferência de linha de base. Você pode abortar uma transferência quando ela entra 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

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

A ação de aborto não é exibida nas seguintes instâncias:

- Se as configurações do RBAC não permitirem esta ação: por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido: por exemplo, quando você tem um relacionamento entre clusters e o cluster de destino ainda não foi descoberto

Não é possível limpar o ponto de verificação de reinicialização 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 no relacionamento na exibição de topologia da transferência de dados que você deseja abortar e selecione **Abortar**.

A caixa de diálogo Abortar transferência é exibida.

2. Se você quiser limpar o ponto de verificação de reinicialização 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 Abortar transferência é fechada, e o status da operação de aborto é exibido na parte

superior da página de detalhes Volume/Integridade, juntamente com um link para os detalhes do trabalho.

4. **Opcional:** Clique no link **Exibir detalhes** para ir para a página de detalhes do **Trabalho** para obter detalhes adicionais e visualizar o andamento do trabalho.
5. Clique em cada tarefa para visualizar seus detalhes.
6. Clique na seta Voltar no seu navegador para retornar à página de detalhes **Volume / Saúde**.

A operação de aborto é concluída quando todas as tarefas do trabalho são concluídas com sucesso.

Desative um relacionamento de proteção na página Relacionamentos de Volume

Na página Relacionamentos de Volume, você pode desativar um relacionamento de proteção para impedir temporariamente que transferências de dados ocorram. Você pode desativar um relacionamento quando quiser criar uma cópia do Snapshot de um volume de destino do SnapMirror que contém um banco de dados e quiser garantir que seu conteúdo esteja estável durante a operação de cópia do Snapshot.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

A ação de inatividade não é exibida nas seguintes instâncias:

- Se as configurações do RBAC não permitirem esta ação; por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido; por exemplo, quando você tem um relacionamento 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 desativar 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 **Desativar**.

A caixa de diálogo Desativar é exibida.

2. Clique em **Continuar**.

O status do trabalho de inatividade é exibido na parte superior da página de detalhes de Volume/Saúde, junto com um link para os detalhes do trabalho.

3. Clique no link **Ver detalhes** para ir para a página de detalhes do **Trabalho** para obter detalhes adicionais e o andamento do trabalho.
4. **Opcional:** Clique na seta **Voltar** no seu navegador para retornar à página **Relacionamentos de volume**.

O trabalho de inatividade é concluído quando todas as tarefas são concluídas com sucesso.

Desativar uma relação de proteção na página de detalhes de Volume/Saúde

Você pode desativar um relacionamento de proteção para impedir temporariamente que transferências de dados ocorram. Você pode desativar um relacionamento quando quiser criar uma cópia do Snapshot de um volume de destino do SnapMirror que contém um banco de dados e quiser garantir que seu conteúdo esteja estável durante a cópia do Snapshot.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

A ação de inatividade não é exibida nas seguintes instâncias:

- Se as configurações do RBAC não permitirem esta ação, por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido, por exemplo, quando você tem um relacionamento 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 / Integridade**, clique com o botão direito do mouse no relacionamento na exibição de topologia para o relacionamento de proteção que você deseja desativar.
2. Selecione **Quiesce** no menu.
3. Clique em **Sim** para continuar.

O status do trabalho de inatividade é exibido na parte superior da página de detalhes de Volume/Saúde, junto com um link para os detalhes do trabalho.

4. Clique no link **Ver detalhes** para ir para a página de detalhes do **Trabalho** para obter detalhes adicionais e o andamento do trabalho.
5. **Opcional:** Clique na seta Voltar no seu navegador para retornar à página de detalhes **Volume / Saúde**.

O trabalho de inatividade é concluído quando todas as tarefas são concluídas com sucesso.

Interromper um relacionamento SnapMirror na página Relacionamentos de Volume

Você pode quebrar um relacionamento de proteção para interromper transferências de dados entre um volume de origem e um volume de destino em um relacionamento SnapMirror . Você pode romper um relacionamento quando quiser migrar dados, para recuperação de desastres ou para testes de aplicativos. O volume de destino é alterado para um volume de leitura/gravação. Você não pode quebrar um relacionamento SnapVault .

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

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 **Interromper**.

A caixa de diálogo Romper relacionamento é exibida.

2. Clique em **Continuar** para encerrar o relacionamento.
3. Na página **Relacionamentos de Volume**, verifique na coluna **Estado do Relacionamento** se o relacionamento foi quebrado.

A coluna Estado do Relacionamento fica oculta por padrão, então talvez seja necessário selecioná-la na lista de colunas mostrar/ocultar .

Remover um relacionamento de proteção da página Relacionamentos de Volume

Na página Relacionamentos de Volume, você pode remover um relacionamento de proteção para excluir permanentemente um relacionamento existente entre a origem e o destino selecionados: por exemplo, quando você deseja criar um relacionamento usando um destino diferente. Esta operação remove todos os metadados e não pode ser desfeita.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

Passos

1. Na página **Relacionamentos de Volume**, selecione um ou mais volumes com relacionamentos de proteção que você 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.

O relacionamento é removido da página Relacionamentos de Volume.

Retomar transferências agendadas em um relacionamento desativado na página Relacionamentos de Volume

Depois de encerrar um relacionamento para impedir que transferências agendadas ocorram, você pode usar **Retomar** para reativar as transferências agendadas para que os dados no volume de origem ou primário sejam protegidos. As transferências são retomadas a partir de um ponto de verificação, se houver, no próximo intervalo de transferência agendado.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

Você pode selecionar no máximo 10 relacionamentos desativados para retomar as transferências.

Passos

1. Na página **Relacionamentos** de Volume, selecione um ou mais volumes com relacionamentos desativados e, na barra de ferramentas, clique em **Retomar**.
2. Na caixa de diálogo **Continuar**, clique em **Continuar**.

Você retornará à página Relacionamentos de Volume.

3. Para visualizar as tarefas relacionadas e acompanhar seu progresso, clique no link da tarefa exibido na parte superior da página **Relacionamentos de volume**.
4. Faça um dos seguintes:
 - Se apenas um trabalho for exibido, na página Detalhes do trabalho, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes das tarefas associadas ao trabalho de configuração de proteção e para determinar quando o trabalho será concluído.
 - Se mais de um trabalho for exibido,
 - i. Na página Trabalhos, clique no trabalho cujos detalhes você deseja visualizar.
 - ii. Na página Detalhes do trabalho, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes das tarefas associadas ao trabalho de configuração de proteção e para determinar quando o trabalho será concluído. Após a conclusão dos trabalhos, as transferências de dados serão retomadas no próximo intervalo de transferência agendado.

Retomar transferências agendadas em um relacionamento desativado na página de detalhes de Volume/Saúde

Depois de encerrar um relacionamento para impedir que transferências agendadas ocorram, você pode usar **Retomar** na página Detalhes do volume/saúde para reativar as transferências agendadas para que os dados no volume de origem ou primário sejam protegidos. As transferências são retomadas a partir de um ponto de verificação, se houver, no próximo intervalo de transferência agendado.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, clique com o botão direito do mouse na exibição de topologia em um relacionamento desativado que você deseja retomar.

Como alternativa, selecione **Retomar** no menu **Ações > Relacionamento**.

2. Na caixa de diálogo **Continuar**, clique em **Continuar**.

Você retornará à página de detalhes de Volume/Saúde.

3. Para visualizar as tarefas relacionadas e acompanhar seu progresso, clique no link da tarefa 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 das tarefas associadas ao trabalho de configuração de proteção e para determinar quando o trabalho será

concluído.

Após a conclusão dos trabalhos, as transferências de dados serão retomadas no próximo intervalo de transferência agendado.

Inicializar ou atualizar relacionamentos de proteção na 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.



Você não pode inicializar ou atualizar volumes protegidos por Grupos de Consistência.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve 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, em seguida, na barra de ferramentas, clique em **Inicializar/Atualizar**.

A caixa de diálogo **Inicializar/Atualizar** é exibida.

2. Na aba **Opções de transferência**, selecione uma prioridade de transferência e a taxa máxima de transferência.
3. Clique em **Cópias de instantâneo de origem**; em seguida, na coluna **Cópia de instantâneo**, clique em **Padrão**.

A caixa de diálogo Selecionar cópia do instantâneo de origem é exibida.

4. Se você quiser especificar uma cópia de Snapshot existente em vez de transferir a cópia de Snapshot padrão, clique em **Cópia de Snapshot existente** e selecione uma cópia de Snapshot na lista.
5. Clique em **Enviar**.

Você retornará à caixa de diálogo **Inicializar/Atualizar**.

6. Se você selecionou mais de uma fonte para inicializar ou atualizar, clique em **Padrão** para a próxima fonte para a qual deseja especificar uma cópia de 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 de 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 trabalho de inicialização ou atualização.

Uma lista filtrada de trabalhos é exibida.

9. **Opcional:** Clique em cada trabalho para ver seus detalhes.
10. **Opcional:** Clique na seta **Voltar** no seu navegador para retornar à página **Relacionamentos de volume**.

A operação de inicialização ou atualização é concluída quando todas as tarefas são concluídas com sucesso.

Inicializar ou atualizar relacionamentos de proteção na 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 você quiser executar uma atualização incremental manual e não programada para transferir dados imediatamente.

OBSERVAÇÃO: Você não pode inicializar ou atualizar volumes protegidos por Grupos de Consistência.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado o OnCommand Workflow Automation.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, localize na topologia o relacionamento de proteção que você deseja inicializar ou atualizar e clique com o botão direito do mouse nele.
2. Selecione **Inicializar/Atualizar** no menu.

Como alternativa, no menu **Ações**, selecione **Relacionamento > Inicializar/Atualizar** para inicializar ou atualizar o relacionamento cujos detalhes você está visualizando no momento.

A caixa de diálogo Inicializar/Atualizar é exibida.

3. Na aba **Opções de transferência**, selecione uma prioridade de transferência e a taxa máxima de transferência.
4. Clique em **Cópias de instantâneo de origem**; em seguida, na coluna **Cópia de instantâneo**, clique em **Padrão**.

A caixa de diálogo Selecionar cópia do instantâneo de origem é exibida.

5. Se você quiser especificar uma cópia de Snapshot existente em vez de transferir a cópia de Snapshot padrão, clique em **Cópia de Snapshot existente** e selecione uma cópia de Snapshot na lista.
6. Clique em **Enviar**.

Você retornará à caixa de diálogo Inicializar/Atualizar.

7. Se você selecionou mais de uma fonte para inicializar ou atualizar, clique em **Padrão** para a próxima fonte de leitura/gravação para a qual deseja especificar uma cópia de Snapshot existente.

Não é possível selecionar uma cópia de 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 do Volume/Saúde

e um link de 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 trabalho de inicialização ou atualização.

Uma lista filtrada de trabalhos é exibida.

10. **Opcional:** Clique em cada trabalho para ver seus detalhes.
11. **Opcional:** Clique na seta Voltar no seu navegador para retornar à página de detalhes **Volume / Saúde**.

A operação de inicialização ou atualização é concluída quando todas as tarefas do trabalho são concluídas com sucesso.

Ressincronizar relacionamentos de proteção na página Relacionamentos de Volume

Na página Relacionamentos de Volume, você pode ressincronizar um relacionamento para se recuperar de um evento que desabilitou seu volume de origem ou quando quiser alterar a origem atual para um volume diferente.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

Passos

1. Na página **Relacionamentos de Volume**, selecione um ou mais volumes com relacionamentos desativados e, na barra de ferramentas, clique em **Ressincronizar**.

A caixa de diálogo Ressincronizar é exibida.

2. Na aba **Opções de ressincronização**, selecione uma prioridade de transferência e a taxa máxima de transferência.
3. Clique em **Cópias de instantâneo de origem**; em seguida, na coluna **Cópia de instantâneo**, clique em **Padrão**.

A caixa de diálogo Selecionar cópia do instantâneo de origem é exibida.

4. Se você quiser especificar uma cópia de Snapshot existente em vez de transferir a cópia de Snapshot padrão, clique em **Cópia de Snapshot existente** e selecione uma cópia de Snapshot na lista.
5. Clique em **Enviar**.

Você retornará à caixa de diálogo Ressincronizar.

6. Se você selecionou mais de uma fonte para ressincronizar, clique em **Padrão** para a próxima fonte para a qual deseja especificar uma cópia de 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 de 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 resincronização.

Uma lista filtrada de trabalhos é exibida.

9. **Opcional:** Clique na seta **Voltar** no seu navegador para retornar à página **Relacionamentos de volume**.

A operação de resincronização é concluída quando todas as tarefas do trabalho são concluídas com sucesso.

Relações de proteção reversa na página Relações de Volume

Quando um desastre desabilita o volume de origem no seu relacionamento de proteção, você pode usar o volume de destino para fornecer dados, convertendo-o em um volume de leitura/gravação enquanto repara ou substitui a origem. Quando a origem estiver novamente disponível para receber dados, você poderá usar a operação de resincronização reversa para estabelecer o relacionamento na direção reversa, sincronizando os dados na origem com os dados no destino de leitura/gravação.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.
- 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 quanto o destino devem estar online.
- A origem não deve ser o destino de outro volume de proteção de dados.
- Ao executar esta tarefa, os dados na origem que são mais recentes que os dados na cópia comum do Snapshot são excluídos.
- As políticas e programações criadas em relacionamentos de resincronização reversa são as mesmas que aquelas no relacionamento de proteção original.

Se políticas e cronogramas não existirem, eles serão criados.

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 **Ressincronização reversa**.

A caixa de diálogo Ressincronização reversa é exibida.

2. Verifique se os relacionamentos exibidos na caixa de diálogo **Ressincronização reversa** são aqueles para os quais você deseja executar a operação de resincronização reversa e clique em **Enviar**.

A operação de resincronização reversa é iniciada, você retorna à página Relacionamentos de Volume e um link de tarefas é exibido na parte superior da página.

3. **Opcional:** Clique em **Exibir trabalhos** na página **Relacionamentos de volume** para rastrear o status de cada trabalho de resincronização reversa.

Uma lista filtrada de trabalhos relacionados a esta operação é exibida.

4. **Opcional:** Clique na seta **Voltar** no seu navegador para retornar à página **Relacionamentos de volume**.

A operação de resincronização reversa é concluída quando todas as tarefas do trabalho são concluídas com sucesso.

Restaurar dados usando as páginas Volume e Detalhes do Volume/Saúde

Você pode restaurar arquivos, diretórios ou um volume inteiro substituídos ou excluídos de uma cópia do Snapshot usando o recurso de restauração nas páginas de detalhes Volume e Volume/Integridade.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.



Observe os seguintes pontos:

- Não é possível restaurar fluxos de arquivos NTFS.
- A opção de restauração não está disponível quando:
 - O ID do volume é desconhecido: por exemplo, quando você tem um relacionamento entre clusters e o cluster de destino ainda não foi descoberto.
 - O volume está configurado para replicação síncrona do SnapMirror .

Passos

1. No painel de navegação esquerdo, vá para **Armazenamento > Volumes**.
2. Selecione o volume e clique no botão **Restaurar**. Como alternativa, clique no volume para acessar **Volume / Detalhes de integridade > Ações > Restaurar**. A caixa de diálogo Restaurar é exibida. Para obter informações sobre esta página, consulte "[Caixa de diálogo Restaurar](#)".
3. Selecione o volume e a cópia do Snapshot dos quais você deseja restaurar os dados, se diferente do padrão.
4. Selecione os itens que deseja restaurar, por exemplo, o LUN de origem.

Você pode restaurar o volume inteiro ou especificar pastas e arquivos que deseja restaurar.

5. Selecione o local onde você deseja que os itens selecionados sejam restaurados: **Local original** ou **Local alternativo existente**.
6. Se você selecionar um local alternativo existente, faça um dos seguintes:
 - No campo de texto Caminho de restauração, digite o caminho do local para o qual você deseja restaurar os dados e clique em **Selecionar diretório**.
 - Clique em **Navegar** para abrir a caixa de diálogo Procurar diretórios e concluir as seguintes etapas:
 - i. Selecione o cluster de destino, a VM de armazenamento (SVM) e o volume para os quais você deseja restaurar.
 - ii. Na tabela Nome, selecione um nome de diretório que deve ser restaurado.
 - iii. Clique em **Selecionar diretório**.
7. Clique em **Restaurar**.

O processo de restauração é iniciado. Um trabalho é criado no backend para concluir o processo de restauração.

8. Se quiser visualizar o andamento do trabalho, no painel de navegação esquerdo, navegue até **Proteção > Trabalhos** para visualizar o status do trabalho de restauração na lista de trabalhos.



Se uma operação de restauração falhar entre clusters do Cloud Volumes ONTAP HA com um erro NDMP, talvez seja necessário adicionar uma rota AWS explícita no cluster de destino para que o destino possa se comunicar com o LIF de gerenciamento de cluster do sistema de origem. Você executa esta etapa de configuração usando o NetApp Console.

O que são pools de recursos

Pools de recursos são grupos de agregados criados por um administrador de armazenamento usando o Unified Manager para fornecer provisionamento a aplicativos parceiros para gerenciamento de backup.

Você pode reunir seus recursos com base em atributos como desempenho, custo, localização física ou disponibilidade. Ao agrupar recursos relacionados em um pool, você pode tratá-lo como uma única unidade para monitoramento e provisionamento. Isso simplifica o gerenciamento desses recursos e permite um uso mais flexível e eficiente do armazenamento.

Durante o provisionamento de armazenamento 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 raiz) e está ONLINE.
- O agregado está em um nó de cluster de destino cuja versão do ONTAP é igual ou superior à 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 fica dentro do limite quase cheio e quase supercomprometido 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.

Criar pools de recursos

Você pode usar a caixa de diálogo Criar pool de recursos para agrupar agregados para fins de provisionamento.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

Os pools de recursos podem conter agregados de diferentes clusters, 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.

Editar pools de recursos

Você pode editar um pool de recursos existente quando quiser alterar o nome e a descrição do pool de recursos.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

O botão **Editar** é habilitado somente quando um pool de recursos é selecionado. Se mais de um pool de recursos for selecionado, o botão **Editar** será desabilitado.

Passos

1. No painel de navegação esquerdo, clique em **Proteção > Pools de recursos**.
2. Selecione um pool de recursos da 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 a descrição são exibidos na lista do pool de recursos.

Ver inventário de pools de recursos

Você pode usar a página Pools de recursos para visualizar o inventário do pool de recursos e monitorar a capacidade restante de cada pool de recursos.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Etapas

1. No painel de navegação esquerdo, clique em **Proteção > Pools de recursos**.

O inventário do pool de recursos é exibido.

Adicionar 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 provisionamento de volume secundário.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você não pode adicionar mais de 200 agregados a um pool de recursos ao mesmo tempo. 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 do pool de recursos.

3. Na área de membros do pool de recursos, clique em **Adicionar**.

A caixa de diálogo Agregados é exibida.

4. Selecione um ou mais agregados.
5. Clique em **Adicionar**.

A caixa de diálogo é fechada e os agregados são exibidos na lista de membros do pool de recursos selecionado.

Remover agregados de pools de recursos

Você pode remover agregados de um pool de recursos existente: por exemplo, quando quiser usar um agregado para alguma outra finalidade.

Antes de começar

Você deve ter a função de Administrador de Aplicativos 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 **Remover** está habilitado.

4. Clique em **Remover**.

Uma caixa de diálogo de aviso é exibida.

5. Clique em **Sim** para continuar.

Os agregados selecionados são removidos do painel Membros.

Excluir 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

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

O botão **Excluir** é habilitado somente quando pelo menos 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 que você deseja excluir.
3. Clique em **Excluir**.

O pool de recursos é removido da lista de pools de recursos e seus agregados são removidos da lista de membros.

Monitorar relacionamentos de proteção de recuperação de desastres de VM de armazenamento

O Active IQ Unified Manager oferece suporte ao monitoramento de relacionamentos de recuperação de desastres de VM de armazenamento, o que fornece recuperação de desastres na granularidade de um nível de VM de armazenamento. 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.

Um relacionamento DR de VM de armazenamento é criado da VM de armazenamento de origem para a VM de armazenamento de destino para fornecer recuperação de desastres assíncrona. Você pode selecionar replicar toda ou um subconjunto da configuração da VM de armazenamento (excluindo a configuração de rede e protocolo) junto com os volumes de dados com base 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 uma 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 origem é reiniciada para fornecer dados. Você pode usar comandos do SnapMirror para configurar e gerenciar o relacionamento de recuperação de desastres da VM de armazenamento.

Monitorar VMs de armazenamento usando a página Relacionamentos

Você pode monitorar os relacionamentos de recuperação de desastres da sua VM de armazenamento na página Relacionamentos na seção PROTEÇÃO do INVENTÁRIO. Por padrão, a página Relacionamentos lista apenas os relacionamentos de nível superior, já que o filtro de relacionamentos constituintes é aplicado.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use filtros para visualizar os relacionamentos de recuperação de desastres da VM de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **PROTEÇÃO > Relacionamentos**.

A página exibe todos os tipos de relacionamentos: volume, grupo de consistência e relacionamentos de VM de armazenamento.

2. Clique em **Filtro** e selecione **Tipo de objeto de relacionamento** e **VM de armazenamento** para visualizar apenas os relacionamentos de recuperação de desastres da VM de armazenamento.
3. Clique em **Aplicar filtro**.



Você deve limpar o filtro de relacionamentos constituintes para visualizar todos os relacionamentos de proteção.

A página exibe apenas relacionamentos de recuperação de desastres de VM de armazenamento.

Exibir relacionamentos de proteção na página VMs de armazenamento

Usando a página VMs de armazenamento, você pode visualizar o status dos relacionamentos de recuperação de desastres das VMs de armazenamento existentes.

Antes de começar

Você deve ter a função de Administrador de Aplicativos 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 baixar 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 **ARMAZENAMENTO > VMs de armazenamento**.
2. No menu **VISUALIZAR**, selecione **Relacionamento > Todos os Relacionamentos**.

A exibição Relacionamento: Todos os relacionamentos é exibida com todas as VMs de armazenamento configuradas.

Exibir VMs de armazenamento com base no status de proteção

Você pode usar a página VMs de armazenamento do Inventário para visualizar todas as VMs de armazenamento no Active IQ Unified Manager e filtrar as VMs de armazenamento com base em seu status de proteção.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Uma nova coluna Função de proteção é adicionada à exibição de VMs de armazenamento que fornece informações sobre se a VM de armazenamento está protegida ou desprotegida.



Se um cluster de origem não for adicionado ao Active IQ Unified Manager, todas as informações relacionadas a esse cluster ficarão indisponíveis nas grades.

Passos

1. No painel de navegação esquerdo, clique em **ARMAZENAMENTO > VMs de armazenamento**.

2. No menu **EXIBIR**, selecione **Saúde > Todas as VMs de armazenamento**.

A tela Saúde: Todas as VMs de armazenamento é exibida.

3. Clique em **Filtro** para visualizar uma das seguintes VMs de armazenamento.

Para visualizar	Valor do filtro
VMs de armazenamento protegidas	Função de Proteção é Protegida
VMs de armazenamento desprotegidas	Função de Proteção é Desprotegida



Não é possível visualizar as VMs de armazenamento protegidas e desprotegidas ao mesmo tempo. Você precisará limpar o filtro existente para reaplicar uma nova opção de filtro.

4. Clique em **Aplicar filtro**.

A exibição Não salva exibe todas as VMs de armazenamento que estão protegidas ou desprotegidas pela recuperação de desastres da VM de armazenamento com base nas suas seleções de filtro.

Entenda as 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 usadas por aplicativos parceiros para seleção de recursos e provisionamento de volume secundário.

As 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 terciário. Não é possível usar uma VM de armazenamento de destino secundária como uma origem para criar uma associação com uma VM de armazenamento de destino terciária.

Como administrador de aplicativos 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 uma ou mais SVMs de destino. Isso significa que todos os SVMs existentes que atualmente exigem proteção, bem como quaisquer SVMs que sejam criados no futuro, estão associados aos SVMs de destino especificados. Por exemplo, você pode querer que aplicativos de diversas fontes diferentes em locais diferentes sejam copiados para uma ou mais SVMs de destino em um único local.
- **Associar uma VM de armazenamento específica:** você pode criar uma associação entre uma VM de armazenamento de origem específica e uma ou mais SVMs de destino específicas. Por exemplo, se você estiver fornecendo serviços de armazenamento para muitos clientes cujos dados devem ser separados uns dos outros, você pode escolher esta opção para associar uma VM de armazenamento de origem específica a uma VM de armazenamento de destino específica que seja atribuída somente 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.

Criar associações de VM de armazenamento

O assistente Criar associações de máquina virtual 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 parceiros usam essas associações no momento do provisionamento inicial dos volumes de destino para determinar quais recursos selecionar.

Antes de começar

- A VM de armazenamento que você está associando já deve existir.
- Você deve ter a função de Administrador de Aplicativos 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 futuras operações 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 **Criar associações de máquinas virtuais de armazenamento** é iniciado.

3. Selecione uma das seguintes fontes:

- **Qualquer**

Escolha esta opção quando quiser criar uma associação entre qualquer origem de VM de armazenamento primário e uma ou mais VMs de armazenamento de destino. Isso significa que todas as VMs de armazenamento existentes que atualmente exigem proteção, bem como quaisquer VMs de armazenamento que sejam criadas no futuro, são associadas à VM de armazenamento de destino especificada. Por exemplo, você pode querer que aplicativos de diversas fontes diferentes em locais diferentes sejam copiados para uma ou mais VMs de armazenamento de destino em um único local.

- **Solteiro**

Escolha esta opção quando quiser selecionar uma VM de armazenamento de origem específica associada a uma ou mais VMs de armazenamento de destino. Por exemplo, se você estiver fornecendo serviços de armazenamento para muitos clientes cujos dados devem ser separados uns dos outros, escolha esta opção para associar uma origem de VM de armazenamento específica a um destino de VM de armazenamento específico que seja atribuído somente a esse cliente.

- **Nenhum (Externo)**

Escolha esta 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 relacionamento de proteção que você deseja criar:

- * SnapMirror*
- * SnapVault*

5. Clique em **Avançar**.

6. Selecione um ou mais destinos de proteção de VM de armazenamento.

7. Clique em **Concluir**.

Excluir associações de VM de armazenamento

Você pode excluir associações de VM de armazenamento para aplicativos parceiros para remover o relacionamento de provisionamento secundário entre as VMs de armazenamento de origem e de destino; por exemplo, você pode fazer isso quando a VM de armazenamento de destino estiver cheia e você quiser criar novas associações de proteção de VM de armazenamento.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

O botão **Excluir** fica desabilitado até que pelo menos uma associação de VM de armazenamento seja selecionada. Alterar associações usando as funções delete e create afeta apenas operações de provisionamento futuras; 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 **Excluir** está habilitado.

3. Clique em **Excluir**.

Uma caixa de diálogo de aviso é exibida.

4. Clique em **Sim** para continuar.

A associação de VM de armazenamento selecionada é removida da lista.

Requisitos de SVM e pool de recursos para oferecer suporte a serviços de armazenamento

Você pode garantir melhor a conformidade em aplicativos parceiros se observar alguns requisitos de associação de SVM e pool de recursos específicos para serviços de armazenamento: por exemplo, quando você associa SVM e cria pools de recursos no Unified Manager para dar suporte a uma topologia de proteção em um serviço de armazenamento fornecido por um aplicativo parceiro.

Alguns aplicativos fazem parceria com o servidor Unified Manager para fornecer serviços que configuram e executam automaticamente a 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 armazenamento de proteção, você deve usar o Unified Manager para configurar as associações SVM e os pools de recursos necessários.

Para oferecer suporte à proteção em cascata ou de salto único do serviço de armazenamento, incluindo replicação de um volume de origem do SnapMirror ou de um volume primário do 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 de SVM devem ser configuradas entre o SVM que contém o volume de origem do SnapMirror ou o volume primário do SnapVault e qualquer SVM no qual resida um volume secundário ou

terciário.

- Por exemplo, para dar suporte a uma topologia de proteção na qual o volume de origem Vol_A reside em SVM_1, o volume de destino secundário do SnapMirror Vol_B reside em SVM_2 e o volume de backup terciário do SnapVault Vol_C reside em SVM_3, você deve usar a interface de usuário da Web do Unified Manager para configurar uma associação do SnapMirror entre SVM_1 e SVM_2 e uma associação de backup do SnapVault entre SVM_1 e SVM_3.

Neste exemplo, qualquer associação SnapMirror ou associação de backup 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 SnapMirror Vol_B residem em SVM_1, você deve configurar uma associação SnapMirror entre SVM_1 e SVM_1.
- Os pools de recursos devem incluir recursos agregados de cluster disponíveis para as SVMs associadas.

Você configura pools de recursos por meio da interface de usuário da Web do Unified Manager e, em seguida, atribui, por meio do aplicativo parceiro, os nós de destino secundário e terciário do serviço de armazenamento.

Quais são os empregos

Um trabalho é uma série de tarefas que você pode monitorar usando o Unified Manager. Visualizar os trabalhos e suas tarefas associadas permite que você determine se eles foram concluídos com sucesso.

Os trabalhos são iniciados quando você cria relacionamentos SnapMirror e SnapVault, quando você executa qualquer operação de relacionamento (interromper, editar, desativar, remover, retomar, ressincronizar e ressincronizar reversamente), quando você executa tarefas de restauração de dados, quando você efetua login em um cluster e assim por diante.

Ao iniciar um trabalho, você pode usar a página Trabalhos e a página Detalhes do trabalho para monitorar o trabalho e o progresso das tarefas associadas.

Monitorar trabalhos

Você pode usar a página Tarefas para monitorar o status da tarefa e visualizar propriedades da tarefa, como tipo de serviço de armazenamento, estado, hora de envio e hora de conclusão, para determinar se uma tarefa foi concluída com sucesso ou não.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Proteção > Trabalhos**.

A página Trabalhos é exibida.

2. Veja a coluna **Estado** para determinar o status dos trabalhos em execução no momento.
3. Clique no nome de um trabalho para ver detalhes sobre ele em particular.

A página Detalhes do trabalho é exibida.

Ver detalhes do trabalho

Depois de iniciar um trabalho, você pode acompanhar seu progresso na página Detalhes do trabalho e monitorar as tarefas associadas em busca de possíveis erros.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Proteção > Trabalhos**.
2. Na página Tarefas, clique no nome de uma tarefa na coluna **Nome** para exibir a lista de tarefas associadas à tarefa.
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.

Abortar trabalhos

Você pode usar a página Tarefas para abortar uma tarefa se ela estiver demorando muito para terminar, estiver apresentando muitos erros ou não for mais necessária. Você pode abortar um trabalho somente se seu status e tipo permitirem. Você pode abortar qualquer tarefa em execução.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Proteção > Trabalhos**.
2. Na lista de trabalhos, selecione um trabalho e clique em **Abortar**.
3. No prompt de confirmação, clique em **Sim** para abortar o trabalho selecionado.

Repetir uma tarefa de proteção com falha

Depois de tomar medidas para corrigir uma tarefa de proteção com falha, você pode usar **Repetir** para executar a tarefa novamente. Tentar executar uma tarefa novamente cria uma nova tarefa usando o ID da tarefa original.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Você pode tentar novamente apenas uma tarefa com falha por vez. Selecionar mais de um trabalho desabilita o botão **Repetir**. Somente tarefas do tipo Configuração de Proteção e Operação de Relacionamento de Proteção podem ser repetidas.

Passos

1. No painel de navegação esquerdo, clique em **Proteção > Trabalhos**.
2. Na lista de trabalhos, selecione um único trabalho do tipo Configuração de Proteção ou Operação de Relacionamento de Proteção com falha.

O botão **Repetir** está habilitado.

3. Clique em **Repetir**.

O trabalho é reiniciado.

Descrição das janelas e caixas de diálogo de relacionamentos de proteção

Você pode visualizar e gerenciar detalhes relacionados à proteção, como pools de recursos, associações de SVM e trabalhos de proteção. Você pode usar a página Limites de integridade apropriada para configurar valores de limite de integridade globais 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 que você crie, monitore e gerencie pools de recursos para fins de provisionamento.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Criar**

Inicia a caixa de diálogo Criar pool de recursos, que você pode usar para criar pools de recursos.

- **Editar**

Permite que você edite o nome e a descrição dos pools de recursos que você cria.

- **Excluir**

Permite que você exclua 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 de 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 de 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.

- **Usado %**

Exibe a porcentagem de espaço usada no pool de recursos.

Botões de comando da lista de membros

Os botões de comando da lista de membros permitem que você execute as seguintes tarefas:

- **Adicionar**

Permite que você adicione membros ao pool de recursos.

- **Excluir**

Permite que você exclua um ou mais membros do pool de recursos.

Lista de membros

A lista de 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 de membros. O status pode ser Crítico (❌), Erro (⚠️), Aviso (⚠️), ou Normal (✅).

- **Nome do Agregado**

Exibe o nome do agregado de membros.

- **Estado**

Exibe o estado atual do agregado, que pode ser um dos seguintes:

- Off-line

Acesso de leitura ou gravação não é permitido.

- On-line

É permitido acesso de leitura e gravação aos volumes hospedados neste agregado.

- Restrito

Operações limitadas (como reconstrução de paridade) são permitidas, mas o acesso a dados não é

permitido.

- Criando

O agregado está sendo criado.

- Destruindo

O agregado está sendo destruído.

- Fracassado

O agregado não pode ser colocado on-line.

- Congelado

O agregado (temporariamente) não está atendendo solicitações.

- Inconsistente

O agregado foi marcado como corrompido; você deve entrar em contato com o suporte técnico.

- Ferro restrito

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.

- Quietude

O agregado está sendo silenciado.

- Silenciou

O agregado está inativo.

- Revertido

A reversão de um agregado é concluída.

- Desmontado

O agregado foi desmontado.

- Desmontagem

O agregado está sendo retirado do ar.

- Desconhecido

O agregado é descoberto, mas as informações agregadas ainda não foram recuperadas pelo servidor

do Unified Manager.

Por padrão, esta coluna está oculta.

- **Conjunto**

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) disponível no agregado.

- **Usado %**

Exibe a porcentagem de espaço que é usada 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, esta 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 e excluir agregados desse pool de recursos.

Nome do pool de recursos

As caixas de texto permitem que você adicione as seguintes informações para criar um pool de recursos:

Permite que você especifique um nome de pool de recursos.

Descrição

Permite que você descreva 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 que você execute as seguintes tarefas:

- **Adicionar**

Abre a caixa de diálogo Agregados para que você possa adicionar agregados de um cluster específico ao pool de recursos. Você pode adicionar agregados de diferentes clusters, 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 será habilitado até que as informações sejam inseridas nos campos Nome ou Descrição do pool de recursos.

- **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 que você altere as seguintes informações para o pool de recursos selecionado:

- **Nome do pool de recursos**

Permite que você insira um novo nome.

- **Descrição**

Permite que você insira uma nova descrição.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Salvar**

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 seu pool de recursos.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Adicionar**

Adiciona os agregados selecionados ao pool de recursos. O botão Adicionar não é habilitado até que pelo menos um agregado seja selecionado.

- **Cancelar**

Descarta as alterações e fecha a caixa de diálogo Agregados.

Lista de agregados

A lista Agregados exibe (em formato tabular) os nomes e propriedades dos agregados monitorados.

- **Status**

Exibe o status atual de um volume. O status pode ser Crítico (❌), Erro (⚠️), Aviso (⚠️), ou Normal (✅).

Você pode mover o ponteiro sobre o status para visualizar mais informações sobre o evento ou eventos gerados para o volume.

- **Nome do Agregado**

Exibe o nome do agregado.

- **Estado**

Exibe o estado atual do agregado, que pode ser um dos seguintes:

- Off-line

Acesso de leitura ou gravação não é permitido.

- Restrito

Operações limitadas (como reconstrução de paridade) são permitidas, mas o acesso a dados não é permitido.

- On-line

É permitido acesso de leitura e gravação aos volumes hospedados neste agregado.

- Criando

O agregado está sendo criado.
- Destruindo

O agregado está sendo destruído.
- Fracassado

O agregado não pode ser colocado on-line.
- Congelado

O agregado (temporariamente) não está atendendo solicitações.
- Inconsistente

O agregado foi marcado como corrompido; você deve entrar em contato com o suporte técnico.
- Ferro restrito

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.
- Quietude

O agregado está sendo silenciado.
- Silenciou

O agregado está inativo.
- Revertido

A reversão de um agregado é concluída.
- Desmontado

O agregado está offline.
- Desmontagem

O agregado está sendo retirado do ar.
- Desconhecido

O agregado é descoberto, mas as informações agregadas ainda não foram recuperadas pelo servidor do Unified Manager.

- **Conjunto**

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, esta 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, esta 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, esta coluna está oculta.

- **Disponível %**

Exibe a porcentagem de espaço disponível para dados no agregado. Por padrão, esta coluna está oculta.

- **Usado %**

Exibe a porcentagem de espaço usada pelos dados no agregado.

- **Tipo RAID**

Exibe o tipo de RAID do volume selecionado. O tipo de RAID pode ser RAID0, RAID4, RAID-DP, RAID-TEC ou RAID misto.

Página de empregos

A página Tarefas permite que você visualize o status atual e outras informações sobre todas as tarefas de proteção de aplicativos de parceiros que estão em execução, bem como tarefas que foram concluídas. Você pode usar essas informações para ver quais tarefas ainda estão em execução e se uma tarefa foi bem-sucedida ou falhou.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Abortar**

Aborta o trabalho selecionado. Esta opção só estará disponível se o trabalho selecionado estiver em

execução.

- **Repetir**

Reinicia um trabalho com falha do tipo Configuração de Proteção ou Operação de Relacionamento de Proteção. Você pode tentar novamente apenas uma tarefa com falha por vez. Se mais de uma tarefa com falha for selecionada, o botão **Repetir** será desabilitado. Não é possível tentar novamente trabalhos de serviço de armazenamento com falha.

- **Atualizar**

Atualiza a lista de trabalhos e as informações associadas a eles.

Lista de empregos

A lista de trabalhos exibe, em formato tabular, uma lista dos trabalhos que estão em andamento. Por padrão, a lista exibe apenas os trabalhos gerados na semana anterior. Você pode usar a classificação e filtragem de colunas para personalizar quais trabalhos são exibidos.

- **Status**

Exibe o status atual de um trabalho. O status pode ser Erro () ou Normal () .

- **ID do trabalho**

Exibe o número de identificação do trabalho. Por padrão, esta coluna está oculta.

O número de identificação do trabalho é único e é atribuído pelo servidor quando ele inicia o trabalho. Você pode pesquisar um trabalho específico inserindo o número de identificação do trabalho na caixa de texto fornecida pelo filtro de coluna.

- **Nome**

Exibe o nome do trabalho.

- **Tipo**

Exibe o tipo de trabalho. Os tipos de trabalho são os seguintes:

- **Aquisição de Cluster**

Um trabalho de automação de fluxo de trabalho está redescobrendo um cluster.

- **Configuração de Proteção**

Uma tarefa de proteção inicia fluxos de trabalho de automação de fluxo de trabalho, como agendamentos cron, criação de políticas do SnapMirror e assim por diante.

- **Operação de Relacionamento de Proteção**

Uma tarefa de proteção está executando operações do SnapMirror .

- **Cadeia de fluxo de trabalho de proteção**

Um trabalho de automação de fluxo de trabalho está executando vários fluxos de trabalho.

- **Restaurar**

Uma tarefa de restauração está em execução.

- **Limpar**

A tarefa é limpar artefatos de membros do serviço de armazenamento que não são mais necessários para fins de restauração.

- **Conformar-se**

A tarefa é verificar a configuração dos membros do serviço de armazenamento para garantir que estejam em conformidade.

- **Destruir**

O trabalho está destruindo um serviço de armazenamento.

- **Importar**

O trabalho é importar objetos de armazenamento não gerenciados para um serviço de armazenamento existente.

- **Modificar**

O trabalho é modificar atributos de um serviço de armazenamento existente.

- **Inscriva-se**

O trabalho é inscrever membros em um serviço de armazenamento.

- **Cancelar inscrição**

O trabalho é cancelar a inscrição de membros de um serviço de armazenamento.

- **Atualizar**

Uma tarefa de atualização de proteção está em execução.

- **Configuração WFA**

Uma tarefa de automação de fluxo de trabalho está enviando credenciais de cluster e sincronizando caches de banco de dados.

- **Estado**

Exibe o estado de execução do trabalho. As opções de estado são as seguintes:

- **Abortado**

O trabalho foi abortado.

- **Abortando**

O trabalho está em processo de aborto.

- **Concluído**

O trabalho terminou.

- **Correndo**

O trabalho está em execução.

- **Hora de envio**

Exibe a hora em que o trabalho foi enviado.

- **Duração**

Exibe o tempo que o trabalho levou para ser concluído. Esta coluna é exibida por padrão.

- **Tempo Concluído**

Exibe a hora em que o trabalho foi concluído. Por padrão, esta coluna está oculta.

Página de detalhes do trabalho

A página Detalhes do trabalho permite que você visualize o status e outras informações sobre tarefas específicas de proteção que estão em execução, que estão na fila ou que foram concluídas. Você pode usar essas informações para monitorar o progresso do trabalho de proteção e solucionar falhas no trabalho.

Resumo do trabalho

O resumo do trabalho exibe as seguintes informações:

- ID do trabalho
- Tipo
- Estado
- Tempo de envio
- Tempo Concluído
- Duração

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Atualizar**

Atualiza a lista de tarefas e as propriedades associadas a cada tarefa.

- **Ver vagas**

Retorna para a página Empregos.

Lista de tarefas do trabalho

A lista de tarefas do trabalho exibe em uma tabela todas as tarefas associadas a um trabalho específico e as propriedades relacionadas a cada tarefa.

- **Hora de início**

Exibe o dia e a hora em que a tarefa começou. 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 tarefa específica:

- **Concluído**

A tarefa foi concluída.

- **Na fila**

A tarefa está prestes a ser executada.

- **Correndo**

A tarefa está em execução.

- **Esperando**

Um trabalho foi enviado e algumas tarefas associadas estão aguardando para serem enfileiradas e executadas.

- **Status**

Exibe o status da tarefa:

- **Erro (🚫)**

A tarefa falhou.

- **Normal (✅)**

A tarefa foi bem-sucedida.

- **Ignorado (🔄)**

Uma tarefa falhou, resultando na omissão de tarefas subsequentes.

- **Duração**

Exibe o tempo decorrido desde o início da tarefa.

- **Tempo Concluído**

Exibe o tempo em que a tarefa foi concluída. Por padrão, esta coluna está oculta.

- **ID da tarefa**

Exibe o GUID que identifica uma tarefa individual para um trabalho. A coluna pode ser classificada e filtrada. Por padrão, esta coluna está oculta.

- **Ordem de dependência**

Exibe um inteiro representando a sequência de tarefas em um gráfico, com zero sendo atribuído à primeira tarefa. Por padrão, esta coluna está oculta.

- **Painel de detalhes da tarefa**

Exibe informações adicionais sobre cada tarefa, incluindo o nome da tarefa, a descrição da tarefa e, se a tarefa falhou, o motivo da falha.

- **Painel de mensagens de tarefas**

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 replicação flexível de versão, backup de múltiplas cópias e configurações relacionadas ao espaço em um volume secundário. Você pode usar a caixa de diálogo Configurações secundárias avançadas quando quiser alterar, habilitar ou desabilitar as configurações atuais.

As configurações relacionadas ao espaço maximizam a quantidade de dados armazenados, incluindo o seguinte: desduplicação, compactação de dados, crescimento automático e garantia de espaço.

A caixa de diálogo inclui os seguintes campos:

- **Habilitar replicação flexível de versão**

Habilita o SnapMirror com replicação flexível de versão. A replicação flexível de versão permite a proteção SnapMirror de um volume de origem, mesmo que o volume de destino esteja sendo executado em uma versão do ONTAP anterior à do volume de origem.

- **Habilitar backup**

Se a replicação flexível de versão estiver habilitada, também permitirá que várias cópias do Snapshot dos dados de origem do SnapMirror sejam transferidas e retidas no destino do SnapMirror .

- **Habilitar desduplicação**

Habilita a desduplicação no volume secundário em um relacionamento SnapVault para que blocos de dados duplicados sejam eliminados e, assim, economizar espaço. Você pode usar a desduplicação quando a economia de espaço for de pelo menos 10% e quando a taxa de substituição de dados não for rápida. A desduplicação é frequentemente usada para ambientes virtualizados, compartilhamentos de arquivos e dados de backup. Esta configuração está desabilitada por padrão. Quando ativada, esta operação é iniciada após cada transferência.

- **Habilitar compressão**

Permite a compactação transparente de dados. 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 de sistema suficientes para que a compactação seja concluída fora dos horários de pico. Em um relacionamento SnapVault, essa configuração é desabilitada por padrão. A compactação só estará disponível quando a deduplicação for selecionada.

- **Comprimir em linha**

Permite economia imediata de espaço ao compactar dados antes de gravá-los no disco. Você pode usar a compactação em linha quando seu sistema não tiver mais de 50% de utilização durante os horários de pico e quando o sistema puder acomodar novas gravações e CPU adicional durante os horários de pico. Esta configuração só estará disponível quando “Ativar compactação” estiver selecionado.

- **Habilitar crescimento automático**

Permite que você aumente automaticamente o volume de destino quando a porcentagem de espaço livre estiver abaixo do limite especificado, desde que haja espaço disponível no agregado associado.

- **Tamanho máximo**

Define a porcentagem máxima até a qual um volume pode crescer. O padrão é 20% maior 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 habilitado somente quando a configuração de crescimento automático está habilitada.

- **Incrementar tamanho**

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 sempre sejam bem-sucedidas. A configuração de garantia de espaço pode ser uma das seguintes:

- **Arquivo**
- **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 ao volume de destino, independentemente do conteúdo na origem. A 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 são alocados no destino para o espaço real usado pelos dados do arquivo na origem.

A garantia de espaço é definida como Volume por padrão.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Aplicar**

Salva as configurações de eficiência selecionadas e as aplica quando você clica em **Aplicar** 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 habilitar as configurações de garantia de espaço em um volume de destino. Você pode selecionar configurações avançadas quando a garantia de espaço estiver desabilitada na origem, mas você quer que ela seja habilitada 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 sempre sejam bem-sucedidas. A configuração de garantia de espaço pode ser uma das seguintes:

- Arquivo
- 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 ao volume de destino, independentemente do conteúdo na origem. A 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 são alocados no destino para o espaço real usado pelos dados do 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 a partir de uma cópia específica do Snapshot.

Restaurar de

A área Restaurar de permite que você especifique de onde deseja restaurar os dados.

- **Volume**

Especifica o volume do qual você deseja restaurar os 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 relacionamentos de proteção com o volume no qual você iniciou a ação de restauração.

- **Cópia instantânea**

Especifica qual cópia do Snapshot você deseja usar para restaurar dados. Por padrão, a cópia mais

recente do Snapshot é selecionada. Você também pode selecionar uma cópia diferente do Snapshot na lista suspensa. A lista de cópias do Snapshot muda de acordo com o volume selecionado.

- **Listar no máximo 995 arquivos e diretórios**

Por padrão, no máximo 995 objetos são exibidos na lista. Você pode desmarcar esta caixa de seleção se quiser visualizar todos os objetos dentro do volume selecionado. Esta operação pode levar algum tempo se o número de itens for muito grande.

Selecione itens para restaurar

A área Selecionar itens para restaurar permite que você selecione o volume inteiro ou arquivos e pastas específicos que deseja restaurar. Você pode selecionar no máximo 10 arquivos, pastas ou uma combinação de ambos. Quando o número máximo de itens é selecionado, as caixas de seleção de itens são desabilitadas.

- **Campo de caminho**

Exibe o caminho para os dados que você deseja restaurar. Você pode navegar até a pasta e os arquivos que deseja restaurar ou digitar o caminho. Este campo fica vazio até que você selecione ou digite um caminho. Clicando  depois de escolher um caminho, você sobe um nível na estrutura do diretório.

- **Lista de pastas e arquivos**

Exibe o conteúdo do caminho inserido. Por padrão, a pasta raiz é exibida inicialmente. Clicar no nome de uma 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 em 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, uma mensagem será exibida para indicar que há muitos itens para exibir e, se você prosseguir com a operação, todos os itens na pasta especificada serão restaurados. Você pode desmarcar a caixa de seleção “Listar no máximo 995 arquivos e diretórios” se quiser visualizar todos os objetos dentro do volume selecionado.



Não é possível restaurar fluxos de arquivos NTFS.

Restaurar para

A área Restaurar para permite que você especifique onde deseja restaurar os dados.

- **Localização original em Volume_Name**

Restaura os dados selecionados para o diretório na origem de onde os dados foram originalmente copiados.

- **Local alternativo**

Restaura os dados selecionados para um novo local:

- Caminho de restauração

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 restaurar os dados ou pode inserir o caminho manualmente usando o formato cluster://svm/volume/path.

- Preservar 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 restaurará os dados usando a seguinte estrutura de diretório no destino: /X/Y/Z/A/B/C/myFile.txt.

Botões de comando

Os botões de comando permitem que você execute 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 Navegar por diretórios

Você pode usar a caixa de diálogo Procurar diretórios quando quiser restaurar dados para um diretório em um cluster e SVM que seja diferente da fonte original. O cluster e o volume de origem originais são selecionados por padrão.

A caixa de diálogo Procurar diretórios permite que você selecione o cluster, o SVM, o volume e o caminho do diretório para os quais deseja restaurar os dados.

- **Conjunto**

Lista os destinos de cluster disponíveis para os quais você pode restaurar. Por padrão, o cluster do volume de origem original é selecionado.

- **Lista suspensa SVM**

Lista o SVM 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 padrão, o volume da fonte original é selecionado.

- **Caixa de texto do caminho do arquivo**

Permite que você digite o caminho do arquivo para o qual deseja restaurar os dados. O caminho que você inserir já deve existir.

- **Nome**

Exibe os nomes das pastas disponíveis para o volume selecionado. Clicar em uma pasta na lista Nome exibe as subpastas, se houver alguma. Os arquivos contidos nas pastas não são exibidos. Clicando  depois de selecionar uma pasta, você sobe um nível na estrutura de diretórios.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Selecione o diretório**

Aplica suas seleções e fecha a caixa de diálogo Procurar diretórios. Se nenhum diretório for selecionado, este botão será desabilitado.

- **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 em clusters para garantir que os dados em um volume de origem ou volume primário sejam replicados.

Guia Fonte

- **Visualização de topologia**

Exibe uma representação visual do relacionamento que você está criando. A origem na topologia é destacada por padrão.

- **Informações da fonte**

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 cumulativo

Exibe o tamanho total de todos os volumes de origem selecionados.

- Tamanho do volume cumulativo usado

Exibe o tamanho do 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

Exibe o tipo de volume.

- Tipo SnapLock

Exibe o tipo SnapLock do volume. As opções são Conformidade, Corporativo e Não SnapLock.

- Cópia instantânea

Exibe a cópia do Snapshot usada para a transferência de linha de base. Se o volume de origem for de leitura/gravação, o valor Padrão na coluna Cópia do instantâneo indica que uma nova cópia do instantâneo é criada por padrão e usada para a transferência de linha de base. Se o volume de origem for um volume de proteção de dados, o valor Padrão na coluna Cópia de instantâneo indica que nenhuma nova cópia de instantâneo é criada e todas as cópias de instantâneo existentes são transferidas para o destino. Clicar no valor Cópia do Snapshot exibe uma lista de cópias do Snapshot da qual você pode selecionar uma cópia do Snapshot existente para usar na transferência de linha de base. Não é possível selecionar uma cópia de Snapshot padrão diferente se o tipo de origem for proteção de dados.

Guia SnapMirror

Permite que você especifique um cluster de destino, uma máquina virtual de armazenamento (SVM) e um agregado para um relacionamento de proteção, bem como uma convenção de nomenclatura para destinos ao criar um relacionamento SnapMirror . Você também pode especificar uma política e agendamento do SnapMirror .

- **Visualização de topologia**

Exibe uma representação visual do relacionamento que você está criando. O recurso de destino do SnapMirror na topologia é destacado por padrão.

- **Informações de destino**

Permite selecionar os recursos de destino para um relacionamento de proteção:

- Link avançado

Inicia a caixa de diálogo Configurações avançadas de destino quando você está criando um relacionamento SnapMirror .

- Conjunto

Lista os clusters que estão disponíveis como hosts de destino de proteção. Este campo é obrigatório.

- máquina virtual de armazenamento (SVM)

Lista as SVMs que estão disponíveis no cluster selecionado. Um cluster deve ser selecionado antes que a lista SVM seja preenchida. Este campo é obrigatório.

- Agregar

Lista os agregados que estão disponíveis no SVM selecionado. Um cluster deve ser selecionado antes

que a lista Agregada seja preenchida. Este campo é obrigatório. A lista Agregada exibe as seguintes informações:

- Classificação

Quando vários agregados satisfazem todos os requisitos para um destino, a classificação indica a prioridade na qual o agregado é listado, de acordo com as seguintes condições:

- A. Um agregado localizado em um nó diferente do nó do volume de origem é preferível para permitir a separação do domínio de falhas.
- B. Um agregado em um nó com menos volumes é preferível para permitir o balanceamento de carga entre os nós de um cluster.
- C. Um agregado que tenha mais espaço livre do que outros agregados é preferível para permitir o balanceamento de capacidade. Uma classificação 1 significa que o agregado é o mais preferido de acordo com os três critérios.

- Nome do 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 será destacado em vermelho se sua entrada for inválida. Clicar no link “Visualizar nome” exibe uma prévia da convenção de nomenclatura que você inseriu, e o texto de visualização é atualizado dinamicamente conforme você digita uma convenção de nomenclatura no campo de texto. Um sufixo entre 001 e 999 é anexado ao nome do destino quando o relacionamento é criado, substituindo o nnn exibido no texto de visualização, com 001 sendo atribuído primeiro, 002 atribuído em segundo e assim por diante.

- **Configurações de relacionamento**

Permite que você especifique a taxa máxima de transferência, a política do SnapMirror e a programação que o relacionamento de proteção usa:

- Taxa máxima de transferência

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 básica entre relacionamentos será ilimitada.

- Política do SnapMirror

Especifica a política ONTAP SnapMirror para o relacionamento. O padrão é DPDefault.

- Criar política

Inicia a caixa de diálogo Criar política do SnapMirror , que permite criar e usar uma nova política do SnapMirror .

- Cronograma do SnapMirror

Especifica a política ONTAP SnapMirror para o relacionamento. Os horários disponíveis incluem Nenhum, 5 minutos, 8 horas, diário, por hora e semanal. O padrão é Nenhum, indicando que nenhuma programação está associada ao relacionamento. Relacionamentos sem agendamentos não têm valores de status de atraso, a menos que pertençam a um serviço de armazenamento.

- Criar agendamento

Inicia a caixa de diálogo Criar agendamento, que permite criar um novo agendamento do SnapMirror .

Guia SnapVault

Permite que você especifique um cluster secundário, SVM e agregado para um relacionamento de proteção, bem como uma convenção de nomenclatura para volumes secundários ao criar um relacionamento SnapVault . Você também pode especificar uma política e uma programação do SnapVault .

- **Visualização de topologia**

Exibe uma representação visual do relacionamento que você está criando. O recurso secundário do SnapVault na topologia é destacado por padrão.

- **Informações secundárias**

Permite selecionar os recursos secundários para um relacionamento de proteção:

- Link avançado

Inicia a caixa de diálogo Configurações secundárias avançadas.

- Conjunto

Lista os clusters que estão disponíveis como hosts de proteção secundários. Este campo é obrigatório.

- máquina virtual de armazenamento (SVM)

Lista as SVMs que estão disponíveis no cluster selecionado. Um cluster deve ser selecionado antes que a lista SVM seja preenchida. Este campo é obrigatório.

- Agregar

Lista os agregados que estão disponíveis no SVM selecionado. Um cluster deve ser selecionado antes que a lista Agregada seja preenchida. Este campo é obrigatório. A lista Agregada exibe as seguintes informações:

- Classificação

Quando vários agregados satisfazem todos os requisitos para um destino, a classificação indica a prioridade na qual o agregado é listado, de acordo com as seguintes condições:

- A. Um agregado localizado em um nó diferente do nó do volume primário é preferível para permitir a separação do domínio de falhas.
- B. Um agregado em um nó com menos volumes é preferível para permitir o balanceamento de carga entre os nós de um cluster.
- C. Um agregado que tenha mais espaço livre do que outros agregados é preferível para permitir o balanceamento de capacidade. Uma classificação 1 significa que o agregado é o mais preferido de acordo com os três critérios.

- Nome do 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 será destacado em vermelho se sua entrada for inválida. Clicar no link “Visualizar nome” exibe uma prévia da convenção de nomenclatura que você inseriu, e o texto de visualização é atualizado dinamicamente conforme 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 exibido no texto de visualização, com 001 sendo atribuído primeiro, 002 atribuído em segundo e assim por diante.

- **Configurações de relacionamento**

Permite que você especifique a taxa máxima de transferência, a política do SnapVault e a programação do SnapVault que o relacionamento de proteção usa:

- Taxa máxima de transferência

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 básica entre relacionamentos será ilimitada.

- Política do SnapVault

Especifica a política do ONTAP SnapVault para o relacionamento. O padrão é XDPDefault.

- Criar política

Inicia a caixa de diálogo Criar política do SnapVault , que permite criar e usar uma nova política do SnapVault .

- Agendamento do SnapVault

Especifica o agendamento do ONTAP SnapVault para o relacionamento. Os horários disponíveis incluem Nenhum, 5 minutos, 8 horas, diário, por hora e semanal. O padrão é Nenhum, indicando que nenhuma programação está associada ao relacionamento. Relacionamentos sem agendamentos não têm valores de status de atraso, a menos que pertençam a um serviço de armazenamento.

- Criar agendamento

Inicia a caixa de diálogo Criar agendamento, que permite criar um agendamento do SnapVault .

Botões de comando

Os botões de comando permitem que você execute 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 que você crie um agendamento de proteção básico ou avançado para transferências de relacionamento do SnapMirror e do SnapVault . Você pode criar um novo cronograma para aumentar a frequência das transferências de dados devido às atualizações frequentes de dados ou pode criar um cronograma menos frequente quando os dados mudam com pouca frequência.

Não é possível configurar agendamentos para relacionamentos síncronos do SnapMirror .

- **Grupo de Destinos**

O nome do cluster que você selecionou na guia SnapVault ou SnapMirror da caixa de diálogo Configurar proteção.

- **Nome da programação**

O nome que você fornece para o cronograma. Os nomes das programações podem consistir nos caracteres de A a Z, de a a z, de 0 a 9, bem como em qualquer um dos seguintes caracteres especiais: ! @ # \$ % ^ & * () _ -. Os nomes das programações não podem incluir os seguintes caracteres: < > .

- **Básico ou Avançado**

O modo de programação que você deseja usar.

O modo básico inclui os seguintes elementos:

- Repita

Com que frequência ocorre uma transferência agendada. As opções incluem por hora, diariamente e semanalmente.

- Dia

Quando uma repetição semanal é selecionada, o dia da semana em que uma transferência ocorre.

- Tempo

Quando Diário ou Semanal é selecionado, a hora do dia em que uma transferência ocorre.

O modo avançado inclui os seguintes elementos:

- Meses

Uma lista numérica separada por vírgulas representando 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 representando 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 da semana

Uma lista numérica separada por vírgulas representando 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 ocorrerá somente 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 representando os minutos em uma hora. Os valores válidos são de 0 a 59. Este elemento é obrigatório.

Caixa de diálogo Criar política do SnapMirror

A caixa de diálogo Criar política do SnapMirror permite que você crie uma política para definir a prioridade das transferências do SnapMirror. Você usa políticas para maximizar a eficiência das transferências da origem para o destino.

- **Grupo de Destinos**

O nome do cluster que você selecionou na guia SnapMirror da caixa de diálogo Configurar proteção.

- **Destino SVM**

O nome do SVM que você selecionou na guia SnapMirror da caixa de diálogo Configurar proteção.

- **Nome da Política**

O nome que você fornece para a nova política. Os nomes de políticas podem consistir nos caracteres de A a Z, de a a z, de 0 a 9, ponto (.), hífen (-) e sublinhado (_).

- **Prioridade de transferência**

A prioridade na qual uma transferência é executada para operações assíncronas. Você pode selecionar Normal ou Baixo. Relacionamentos de transferência com políticas que especificam uma prioridade de transferência normal são executados antes daqueles com políticas que especificam uma prioridade de transferência baixa.

- **Comentário**

Um campo opcional no qual você pode adicionar comentários sobre a política.

- **Reinício da transferência**

Indica qual ação de reinicialização tomar quando uma transferência é interrompida por uma operação de aborto ou qualquer tipo de falha, como uma queda de rede. Você pode selecionar uma das seguintes opções:

- Sempre

Especifica que uma nova cópia do Snapshot é criada antes de reiniciar uma transferência. Então, se houver uma, a transferência é reiniciada a partir de um ponto de verificação, seguida por uma transferência incremental da cópia do Snapshot recém-criada.

- Nunca

Especifica que transferências interrompidas nunca são reiniciadas.

Botões de comando

Os botões de comando permitem que você execute 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 do SnapVault

A caixa de diálogo Criar política do SnapVault permite que você crie uma política para definir a prioridade das transferências do SnapVault . Use políticas para maximizar a eficiência das transferências do volume primário para o secundário.

- **Grupo de Destinos**

O nome do cluster que você selecionou na guia SnapVault da caixa de diálogo Configurar proteção.

- **Destino SVM**

O nome do SVM que você selecionou na guia SnapVault da caixa de diálogo Configurar proteção.

- **Nome da Política**

O nome que você fornece para a nova política. Os nomes de políticas podem consistir nos caracteres de A a Z, de a a z, de 0 a 9, ponto (.), hífen (-) e sublinhado (_).

- **Prioridade de transferência**

A prioridade na qual a transferência é executada. Você pode selecionar Normal ou Baixo.

Relacionamentos de transferência com políticas que especificam uma prioridade de transferência normal são executados antes daqueles com políticas que especificam uma prioridade de transferência baixa. A configuração padrão é Normal.

- **Comentário**

Um campo opcional no qual você pode adicionar um comentário de até 255 caracteres sobre a política do SnapVault .

- **Ignorar tempo de acesso**

Especifica se as transferências incrementais são ignoradas para arquivos que tiveram apenas o tempo de acesso alterado.

- **Rótulo de replicação**

Lista em uma tabela as regras associadas às cópias de 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 que você execute as seguintes ações:

- Adicionar

Permite que você crie um rótulo de cópia do Snapshot e uma contagem de retenção.

- Editar Contagem de Retenção

Permite que você altere a contagem de retenção de um rótulo de cópia de 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.

- Excluir

Permite que você exclua um rótulo de cópia de Snapshot existente.

- Rótulo de cópia de instantâneo

Exibe o rótulo da cópia do Snapshot. Se você selecionar um ou mais volumes com a mesma política de cópia de Snapshot local, uma entrada para cada rótulo na política será exibida. Se você selecionar vários volumes que tenham duas ou mais políticas de cópia de instantâneo local, a tabela exibirá todos os rótulos de todas as políticas

- Agendar

Exibe a programação associada a cada rótulo de cópia do Snapshot. Se um rótulo tiver mais de uma programação associada, as programações desse rótulo serão exibidas em uma lista separada por vírgulas. Se você selecionar vários volumes com o mesmo rótulo, mas com agendamentos diferentes, o agendamento exibirá "Vários" para indicar que mais de um agendamento está associado aos volumes selecionados.

- Contagem de retenção de destino

Exibe o número de cópias do Snapshot com o rótulo especificado que são retidas no SnapVault secundário. As contagens de retenção para rótulos com vários agendamentos exibem a soma das contagens de retenção de cada par de rótulo e agendamento. Se você selecionar vários volumes com duas ou mais políticas de cópia de Snapshot local, a contagem de retenção ficará vazia.

Caixa de diálogo Editar relacionamento

Você pode editar um relacionamento de proteção existente para alterar a taxa máxima de transferência, a política de proteção ou o cronograma de proteção.

Informações de destino

- **Grupo de Destinos**

O nome do cluster de destino selecionado.

- **Destino SVM**

O nome do SVM selecionado

- **Configurações de relacionamento**

Permite que você especifique a taxa máxima de transferência, a política do SnapMirror e a programação que o relacionamento de proteção usa:

- Taxa máxima de transferência

Especifica a taxa máxima na qual os dados 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 quilobytes por segundo (KBps), megabytes por segundo (MBps), gigabytes por segundo (GBps) ou terabytes por segundo (TBps). A taxa máxima de transferência especificada deve ser maior que 1 KBps e menor que 4 TBps. Se você optar por não usar uma taxa de transferência máxima, a transferência básica entre relacionamentos será ilimitada. Se o cluster primário e o cluster secundário forem iguais, essa configuração será desabilitada.

- Política do SnapMirror

Especifica a política ONTAP SnapMirror para o relacionamento. O padrão é DPDefault.

- Criar política

Inicia a caixa de diálogo Criar política do SnapMirror , que permite criar e usar uma nova política do SnapMirror .

- Cronograma do SnapMirror

Especifica a política ONTAP SnapMirror para o relacionamento. Os horários disponíveis incluem Nenhum, 5 minutos, 8 horas, diário, por hora e semanal. O padrão é Nenhum, indicando que nenhuma programação está associada ao relacionamento. Relacionamentos sem agendamentos não têm valores de status de atraso, a menos que pertençam a um serviço de armazenamento.

- Criar agendamento

Inicia a caixa de diálogo Criar agendamento, que permite criar um novo agendamento do SnapMirror .

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Cancelar**

Descarta as seleções e fecha a caixa de diálogo Configurar proteção.

- **Enviar**

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 desejar executar uma atualização manual, não programada e incremental.

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. Você pode selecionar Normal ou Baixo. Relacionamentos com políticas que especificam uma prioridade de transferência normal são executados antes daquelas que especificam uma prioridade de transferência baixa. Normal é selecionado por padrão.

- **Taxa Máxima de Transferência**

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 básica entre relacionamentos será ilimitada. Se você selecionar mais de um relacionamento com diferentes taxas máximas de transferência, poderá especificar uma das seguintes configurações de taxa máxima de transferência:

- 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 está disponível somente quando vários relacionamentos com diferentes taxas de transferência estão sendo inicializados ou atualizados.

- Ilimitado

Indica que não há limitação de largura de banda nas transferências entre relacionamentos. Este campo está disponível somente quando vários relacionamentos com diferentes taxas de transferência estão sendo inicializados ou atualizados.

- Limitar 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 quilobytes por segundo (KBps), megabytes por segundo (MBps), gigabytes por segundo (GBps) ou terabytes por segundo (TBps). A taxa máxima de transferência especificada deve ser maior que 1 KBps e menor que 4 TBps.

Guia Cópias de instantâneos de origem

A guia Cópias do Snapshot de Origem exibe as seguintes informações sobre a cópia do Snapshot de origem usada para a transferência de linha de base:

- **Volume de origem**

Exibe os nomes dos volumes de origem correspondentes.

- **Volume de destino**

Exibe os nomes dos volumes de destino selecionados.

- **Tipo de fonte**

Exibe o tipo de volume. O tipo pode ser Leitura/gravação ou Proteção de Dados.

- **Cópia instantânea**

Exibe a cópia do Snapshot usada para a transferência de dados. Clicar no valor Cópia de instantâneo exibe a caixa de diálogo Selecionar cópia de instantâneo de origem, na qual você pode selecionar uma cópia de instantâneo específica para sua transferência, dependendo do tipo de relacionamento de proteção que você tem e da operação que está executando. A opção para especificar uma cópia de Snapshot diferente não está disponível para fontes de tipo de proteção de dados.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Cancelar**

Descarta suas seleções e fecha a caixa de diálogo Inicializar/Atualizar.

- **Enviar**

Salva suas seleções e inicia o trabalho de inicialização ou atualização.

Caixa de diálogo Ressincronizar

A caixa de diálogo Ressincronizar permite que você ressincronize dados em um relacionamento SnapMirror ou SnapVault que foi interrompido anteriormente e então o

destino se tornou um volume de leitura/gravação. Você também pode ressincronizar quando uma cópia comum necessária do Snapshot no volume de origem for excluída, causando falha nas atualizações do SnapMirror ou SnapVault .

Guia Opções de ressincronização

A guia Opções de ressincronização permite que você defina a prioridade de transferência e a taxa máxima de transferência para o relacionamento de proteção que você está ressincronizando.

- **Prioridade de transferência**

A prioridade na qual a transferência é executada. Você 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 Máxima de Transferência**

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 básica entre relacionamentos será ilimitada.

Guia Cópias de instantâneos de origem

A guia Cópias do Snapshot de Origem exibe as seguintes informações sobre a cópia do Snapshot de origem usada para a transferência de linha de base:

- **Volume de origem**

Exibe os nomes dos volumes de origem correspondentes.

- **Volume de destino**

Exibe os nomes dos volumes de destino selecionados.

- **Tipo de fonte**

Exibe o tipo de volume: Leitura/gravação ou Proteção de dados.

- **Cópia instantânea**

Exibe a cópia do Snapshot usada para a transferência de dados. Clicar no valor Cópia de instantâneo exibe a caixa de diálogo Selecionar cópia de instantâneo de origem, na qual você pode selecionar uma cópia de instantâneo específica para sua transferência, dependendo do tipo de relacionamento de proteção que você tem e da operação que está executando.

Botões de comando

- **Enviar**

Inicia o processo de ressincronização e fecha a caixa de diálogo Ressincronizar.

- **Cancelar**

Cancela suas seleções e fecha a caixa de diálogo Ressincronizar.

Caixa de diálogo Selecionar cópia do instantâneo de origem

Use a caixa de diálogo Selecionar cópia de instantâneo de origem para selecionar uma cópia de instantâneo 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 que você selecione o comportamento padrão para determinar qual cópia do Snapshot é usada para inicializar, atualizar e ressincronizar transferências para relacionamentos SnapVault e SnapMirror.

Se você estiver realizando uma transferência do SnapVault, o comportamento padrão para cada operação será o seguinte:

Operação	Comportamento padrão do SnapVault quando a origem é de leitura/gravação	Comportamento padrão do SnapVault quando a origem é Proteção de Dados (DP)
Inicializar	Cria uma nova cópia do Snapshot e a transfere.	Transfere a última cópia exportada do Snapshot.
Atualizar	Transfere apenas cópias de Snapshot rotuladas, conforme especificado na política.	Transfere a última cópia exportada do Snapshot.
Ressincronizar	Transfere todas as cópias de Snapshot rotuladas criadas após a cópia de Snapshot comum mais recente.	Transfere a cópia mais recente do Snapshot rotulada.

Se você estiver realizando uma transferência do SnapMirror, o comportamento padrão para cada operação será o seguinte:

Operação	Comportamento padrão do SnapMirror	Comportamento padrão do SnapMirror quando o relacionamento é o segundo salto em uma cascata SnapMirror para SnapMirror
Inicializar	Cria uma nova cópia do Snapshot e a transfere, juntamente com todas as cópias do Snapshot criadas antes da nova cópia do Snapshot.	Transfere todas as cópias do Snapshot da origem.

Operação	Comportamento padrão do SnapMirror	Comportamento padrão do SnapMirror quando o relacionamento é o segundo salto em uma cascata SnapMirror para SnapMirror
Atualizar	Cria uma nova cópia do Snapshot e a transfere, juntamente com todas as cópias do Snapshot criadas antes da nova cópia do Snapshot.	Transfere todas as cópias do Snapshot.
Ressincronizar	Cria uma nova cópia do Snapshot e então transfere todas as cópias do Snapshot da origem.	Transfere todas as cópias do Snapshot do volume secundário para o volume terciário e exclui todos os dados adicionados após a criação da cópia comum mais recente do Snapshot.

Cópia de instantâneo existente

Permite que você selecione uma cópia de Snapshot existente na lista se a seleção de cópia de Snapshot for permitida para essa operação.

- **Cópia instantânea**

Exibe as cópias existentes do Snapshot que você pode selecionar para uma transferência.

- **Data de criação**

Exibe a data e a hora em que a cópia do Snapshot foi criada. As cópias de instantâneos são listadas da mais recente para a menos recente, com a mais recente no topo da lista.

Se você estiver executando uma transferência do SnapVault e quiser selecionar uma cópia existente do Snapshot para transferir de uma origem para um destino, o comportamento de cada operação será o seguinte:

Operação	Comportamento do SnapVault ao especificar uma cópia do Snapshot	Comportamento do SnapVault ao especificar uma cópia do Snapshot em uma cascata
Inicializar	Transfere a cópia do Snapshot especificada.	A seleção de cópias do instantâneo de origem não é suportada para volumes de proteção de dados.
Atualizar	Transfere a cópia do Snapshot especificada.	A seleção de cópias do instantâneo de origem não é suportada para volumes de proteção de dados.

Operação	Comportamento do SnapVault ao especificar uma cópia do Snapshot	Comportamento do SnapVault ao especificar uma cópia do Snapshot em uma cascata
Ressincronizar	Transfere a cópia do Snapshot selecionada.	A seleção de cópias do instantâneo de origem não é suportada para volumes de proteção de dados.

Se você estiver executando uma transferência do SnapMirror e quiser selecionar uma cópia do Snapshot existente para transferir de uma origem para um destino, o comportamento de cada operação será o seguinte:

Operação	Comportamento do SnapMirror ao especificar uma cópia do Snapshot	Comportamento do SnapMirror ao especificar uma cópia do Snapshot em uma cascata
Inicializar	Transfere todas as cópias do Snapshot na origem, até a cópia do Snapshot especificada.	A seleção de cópias do instantâneo de origem não é suportada para volumes de proteção de dados.
Atualizar	Transfere todas as cópias do Snapshot na origem, até a cópia do Snapshot especificada.	A seleção de cópias do instantâneo de origem não é suportada para volumes de proteção de dados.
Ressincronizar	Transfere todas as cópias do Snapshot da origem, até a cópia do Snapshot selecionada, e então exclui todos os dados adicionados após a criação da cópia comum mais recente do Snapshot.	A seleção de cópias do instantâneo de origem não é suportada para volumes de proteção de dados.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Enviar**

Envia suas seleções e fecha a caixa de diálogo Selecionar cópia de instantâneo de origem.

- **Cancelar**

Descarta suas seleções e fecha a caixa de diálogo Selecionar cópia de instantâneo de origem.

Caixa de diálogo Ressincronização reversa

Quando você tem um relacionamento de proteção que é quebrado porque o volume de origem está desabilitado e o destino se torna um volume de leitura/gravação, a ressincronização reversa permite que você inverta a direção do relacionamento para que o destino se torne a nova origem e a origem se torne o novo destino.

Quando um desastre desabilita o volume de origem no seu relacionamento de proteção, você pode usar o volume de destino para fornecer dados convertendo-os para leitura/gravação, enquanto repara ou substitui a

origem, atualiza a origem e restabelece o relacionamento. Quando você executa uma operação de ressincronização reversa, os dados na origem que são mais recentes que os dados na cópia comum do Snapshot são excluídos.

Antes da ressincronização reversa

Exibe a origem e o destino de um relacionamento antes de uma operação de ressincronização reversa.

- **Volume de origem**

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 ressincronização reversa.

Após ressincronização reversa

Exibe qual é a origem e o destino de um relacionamento após uma operação de ressincronização de reserva.

- **Volume de origem**

O nome e a localização do volume de origem após uma operação de ressincronização reversa.

- **Volume de destino**

O nome e a localização do volume de destino após uma operação de ressincronização reversa.

Botões de comando

Os botões de comando permitem que você execute as seguintes ações:

- **Enviar**

Inicia o processo de ressincronização reversa.

- **Cancelar**

Fecha a caixa de diálogo Ressincronização reversa sem iniciar uma operação de ressincronização reversa.

Relacionamento: Visualização de todos os relacionamentos

A exibição Relacionamento: Todos os relacionamentos exibe informações sobre relacionamentos de proteção no sistema de armazenamento.

Por padrão, quando você acessa a página Relacionamentos, o relatório exibido inclui os relacionamentos de proteção de nível superior para volumes e VMs de armazenamento. Os controles na parte superior da página permitem que você selecione uma visualização específica, realize pesquisas para localizar objetos específicos, crie e aplique filtros para restringir a lista de dados exibidos, adicione/remova/reordene colunas na página e exporte 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 então 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 relacionamentos de proteção para volumes e VMs de

armazenamento no seu datacenter. Você pode usar a opção **Filtro** 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 quiser visualizar relacionamentos de VM de volume ou de armazenamento, você pode acessar a página **Armazenamento > 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 dados de volumes ou VMs de armazenamento.

A página Relacionamentos que lista todos os relacionamentos de proteção tem o link **Exibir no Gerenciador de Sistema** para o cluster de Destino que permite que você visualize os mesmos objetos no Gerenciador de Sistema ONTAP.

- **Status**

Exibe o status atual do relacionamento de proteção.

O status pode ser um de Erro () , Aviso () , ou OK () .

- **VM de armazenamento de origem**

Exibe o nome do SVM de origem. Você pode ver mais detalhes sobre o SVM de origem clicando no nome do SVM.

Quando um SVM existe no cluster, mas ainda não foi adicionado ao inventário do Unified Manager, ou o SVM foi criado após a última atualização do cluster, este campo estará vazio. Você deve garantir que o SVM exista ou executar uma redescoberta no cluster para atualizar a lista de recursos.

- **Fonte**

Exibe o volume de origem ou a VM de armazenamento de origem que está sendo protegida com base na sua seleção. Você pode ver mais detalhes sobre o volume de origem ou a VM de armazenamento clicando no nome do volume ou da VM de armazenamento.

Se a mensagem `Resource-key not discovered` for exibido, isso pode 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 exista ou executar uma redescoberta no cluster para atualizar a lista de recursos.

- **VM de armazenamento de destino**

Exibe o nome do SVM de destino. Você pode ver mais detalhes sobre o SVM de destino clicando 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 de Objeto de Relacionamento**

Exibe o tipo de objeto usado no relacionamento, 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 clicar neles leva você à página LUNs para visualizar o relacionamento.

- **Política**

Exibe o nome da política de proteção para o relacionamento SnapMirror . Você pode clicar no nome da política para visualizar os detalhes associados a ela, 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. Transferências prioritárias normais são agendadas antes de transferências de baixa prioridade. O padrão é Normal.

- Ignorar tempo de acesso

Aplica-se somente aos relacionamentos do SnapVault . Isso especifica se as transferências incrementais ignoram arquivos cujo tempo de acesso foi alterado apenas. Os valores são Verdadeiro ou Falso. O padrão é Falso.

- Quando o relacionamento está fora de sincronia

Especifica a ação que o ONTAP executa quando um relacionamento síncrono não pode ser sincronizado. Os relacionamentos StrictSync restringirão o acesso ao volume primário se houver uma falha de sincronização com o volume secundário. Os relacionamentos de sincronização não restringem o acesso ao primário se houver uma falha de sincronização com o secundário.

- Limite de tentativas

Especifica o número máximo de tentativas de transferência manual ou agendada para um relacionamento SnapMirror . O padrão é 8.

- Comentários

Fornece um campo de texto para comentários específicos da política selecionada.

- Etiqueta SnapMirror

Especifica o rótulo SnapMirror para o primeiro agendamento associado à política de cópia do Snapshot. O rótulo SnapMirror é usado pelo subsistema SnapVault quando você faz backup de cópias do Snapshot para um destino SnapVault .

- Configuração de retenção

Especifica por quanto tempo os backups são mantidos, com base no tempo ou no número de backups.

- Cópias instantâneas reais

Especifica o número de cópias de Snapshot neste volume que correspondem ao rótulo especificado.

- Preservar cópias de instantâneos

Especifica o número de cópias do SnapVault Snapshot 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 cópias do Snapshot no qual um aviso é enviado para indicar que o limite máximo

de retenção está quase atingido.

- **Duração do atraso**

Exibe a quantidade de tempo que os dados no espelho ficam atrasados em relação à origem.

A duração do atraso deve ser próxima ou igual a 0 segundos para relacionamentos StrictSync.

- **Status de atraso**

Exibe o status de atraso para relacionamentos gerenciados e para relacionamentos não gerenciados que têm uma programação associada a esse relacionamento. O status 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 maior 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 para relacionamentos síncronos porque um agendamento não pode ser configurado.

- **Última atualização bem-sucedida**

Exibe a hora da última operação bem-sucedida do SnapMirror ou SnapVault .

A última atualização bem-sucedida não é aplicável para relacionamentos síncronos.

- **Relacionamentos Constituintes**

Exibe se há algum volume no objeto selecionado.

- **Tipo de relacionamento**

Exibe o tipo de relacionamento usado para replicar um volume. Os tipos de relacionamento incluem:

- Espelho Assíncrono
 - Cofre Assíncrono
 - MirrorVault assíncrono
 - Sincronização Estrita
 - Sincronizar

- **Status da transferência**

Exibe o status de transferência do relacionamento de proteção. O status da transferência pode ser um dos seguintes:

- Abortando

As transferências do SnapMirror estão habilitadas; no entanto, uma operação de aborto de transferência que pode incluir a remoção do ponto de verificação está em andamento.

- Verificando

O volume de destino está passando por uma verificação de diagnóstico e nenhuma transferência está em andamento.

- Finalizando

Transferências SnapMirror estão habilitadas. O volume está atualmente na fase de pós-transferência para transferências incrementais do SnapVault .

- Parado

As transferências estão habilitadas e nenhuma transferência está em andamento.

- Em sincronia

Os dados nos dois volumes no relacionamento síncrono são sincronizados.

- Fora de sincronia

Os dados no volume de destino não estão sincronizados com o volume de origem.

- Preparando

Transferências SnapMirror estão habilitadas. O volume está atualmente na fase de pré-transferência para transferências incrementais do SnapVault .

- Na fila

Transferências SnapMirror estão habilitadas. Nenhuma transferência está em andamento.

- Silenciou

As transferências do SnapMirror estão desativadas. Nenhuma transferência está em andamento.

- Quietude

Uma transferência do SnapMirror está em andamento. Transferências adicionais estão desabilitadas.

- Transferindo

As transferências do SnapMirror estão habilitadas e uma transferência está em andamento.

- Transição

A transferência assíncrona de dados do volume de origem para o volume de destino foi concluída e a transição para a operação síncrona foi iniciada.

- Esperando

Uma transferência do SnapMirror foi iniciada, mas algumas tarefas associadas estão aguardando para

serem enfileiradas.

- **Duração da última transferência**

Exibe o tempo necessário para a conclusão da última transferência de dados.

A duração da transferência não é aplicável para relacionamentos StrictSync porque a transferência deve ser simultânea.

- **Tamanho da última transferência**

Exibe o tamanho, em bytes, da última transferência de dados.

O tamanho da transferência não é aplicável para relacionamentos 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 no Unified Manager.

- Endereço IP do mediador

Se estiver configurado, os clusters de origem e destino serão adicionados no Unified Manager.

- **Estado**

Exibe o estado do relacionamento SnapMirror ou SnapVault . O estado pode ser Não Inicializado, SnapMirrored ou Interrompido. Se um volume de origem for selecionado, o estado do relacionamento não será aplicável e não será exibido.

- **Saúde do Relacionamento**

Exibe a integridade do relacionamento do cluster.

- **Motivo Insalubre**

A razão pela qual o relacionamento está em um estado doentio.

- **Prioridade de transferência**

Exibe a prioridade na qual uma transferência é executada. A prioridade de transferência é Normal ou Baixa. Transferências prioritárias normais são agendadas antes de transferências de baixa prioridade.

A prioridade de transferência não é aplicável para relacionamentos síncronos porque todas as transferências são tratadas com a mesma prioridade.

- **Agendar**

Exibe o nome do cronograma de proteção atribuído ao relacionamento.

O cronograma não é aplicável para relacionamentos síncronos.

- **Versão Replicação Flexível**

Exibe Sim, Sim com opção de backup ou Nenhum.

- **Cluster de origem**

Exibe o FQDN, nome abreviado ou endereço IP do cluster de origem para o relacionamento SnapMirror .

- **FQDN do cluster de origem**

Exibe o nome do cluster de origem para o relacionamento SnapMirror .

- **Nó de Origem**

Exibe o nome do link do nome do nó de origem para o relacionamento SnapMirror de um volume e exibe o link da contagem de nós do relacionamento SnapMirror quando o objeto é uma VM de armazenamento ou um grupo de consistência.

Na exibição personalizada, ao clicar no link do nome do nó, você pode visualizar e estender a proteção para objetos de armazenamento nos quais os volumes desses Grupos de Consistência pertencem a um relacionamento de sincronização ativa do SnapMirror .

Ao clicar no link de contagem de nós, você será levado para a página de nós com os respectivos nós associados a esse relacionamento. Quando a contagem de nós é 0, não há valor exibido, pois não há nós associados ao relacionamento.

- **Nó de Destino**

Exibe o nome do link do nome do nó de destino para o relacionamento SnapMirror de um volume e exibe o link da contagem de nós do relacionamento SnapMirror quando o objeto é uma VM de armazenamento ou um grupo de consistência.

Ao clicar no link de contagem de nós, você será levado para a página de nós com os respectivos nós associados a esse relacionamento. Quando a contagem de nós é 0, não há valor exibido, pois não há nós associados ao relacionamento.

- **Grupo de Destinos**

Exibe o nome do cluster de destino para o relacionamento SnapMirror .

- **FQDN do cluster de destino**

Exibe o FQDN, nome abreviado ou endereço IP do cluster de destino para o relacionamento SnapMirror .

- **Protegido por**

Exibe os diferentes relacionamentos. Nesta coluna, você pode visualizar os relacionamentos de volume e grupo de consistência para clusters e ordem de máquinas virtuais de armazenamento, incluindo:

- SnapMirror
- VM de armazenamento DR

- SnapMirror, VM de armazenamento DR
- Grupo de Consistência
- SnapMirror, Grupo de Consistência.

Informações relacionadas

- Para obter informações sobre a visualização **Relacionamento: MetroCluster**, consulte "[Monitoramento das configurações do MetroCluster](#)".
- Para obter informações sobre a visualização **Relacionamento: Status de transferência do último mês**, consulte "[Relacionamento: Visualização do status de transferência do último mês](#)".
- Para obter informações sobre a visualização **Relacionamento: Todos os relacionamentos**, consulte "[Relacionamento: Visualização da taxa de transferência do último mês](#)".

Relacionamento: Visualização do status de transferência do último mês

A exibição **Relacionamento: Status de transferência do último mês** permite que você analise as tendências de transferência ao longo de um período de tempo para volumes e VMs de armazenamento em relacionamentos assíncronos. Esta página também exibe se a transferência foi um sucesso ou uma falha.

Os controles na parte superior da página permitem que você execute pesquisas para localizar objetos específicos, crie e aplique filtros para restringir a lista de dados exibidos, adicionar/remover/reordenar colunas na página e exportar os dados da página para um .csv, .pdf, ou .xlsx arquivo. Depois de personalizar a página, você pode salvar os resultados como uma visualização personalizada e então agendar um relatório desses dados para ser gerado e enviado por e-mail regularmente. Você pode usar a opção **Filtro** 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. Por exemplo, se você quiser visualizar relacionamentos de volume, poderá acessar o relatório **Relacionamento: Status de transferência do último mês** para as VMs de armazenamento no menu **Armazenamento > VMs de armazenamento > Relacionamento: Status de transferência do último mês** ou no menu **Proteção > Relacionamentos > Relacionamento: Status de transferência do último mês** e usar o **Filtro** para visualizar apenas os dados dos volumes.

- **Volume de origem**

Exibe o nome do volume de origem.

- **Volume de destino**

Exibe o nome do volume de destino.

- **Tipo de operação**

Exibe o tipo de transferência de volume.

- **Resultado da Operação**

Exibe se a transferência de volume foi bem-sucedida.

- **Hora de início da transferência**

Exibe a hora de início da transferência de volume.

- **Hora de término da transferência**

Exibe o horário de término da transferência de volume.

- **Duração da transferência**

Exibe 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 armazenamento (SVM).

- **Cluster de origem**

Exibe o nome do cluster de origem.

- **Destino SVM**

Exibe o nome do SVM de destino.

- **Grupo de Destinos**

Exibe o nome do cluster de destino.

Informações relacionadas

- Para obter informações sobre a visualização **Relacionamento: Todos os relacionamentos**, consulte "[Relacionamento: Visualização de todos os relacionamentos](#)".
- Para obter informações sobre a visualização **Relacionamento: MetroCluster**, consulte "[Monitoramento das configurações do MetroCluster](#)".
- Para obter informações sobre a visualização **Relacionamento: Todos os relacionamentos**, consulte "[Relacionamento: Visualização da taxa de transferência do último mês](#)".

Relacionamento: Visualização da taxa de transferência do último mês

A exibição Relacionamento: Taxa de transferência do último mês permite que você analise a quantidade de volume de dados que é transferida diariamente para volumes em relacionamentos assíncronos. Esta página também fornece detalhes sobre transferências diárias e o tempo necessário para concluir a operação de transferência para volumes e VMs de armazenamento.

Os controles na parte superior da página permitem que você execute pesquisas para localizar objetos específicos, crie e aplique filtros para restringir a lista de dados exibidos, adicione/remova/reordene colunas na página e exporte 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 então agendar um relatório desses dados para ser gerado e enviado por e-mail regularmente. Por exemplo, se você quiser visualizar relacionamentos de volume, você pode acessar o menu **Armazenamento > Volumes > Relacionamento: Taxa de transferência do último mês** ou acessar o menu **Proteção > Relacionamentos > Relacionamentos: Taxa de transferência do último mês** e usar o **Filtro** para visualizar somente dados de

volumes.

- **Tamanho total da transferência**

Exibe o tamanho total da transferência de volume em gigabytes.

- **Dia**

Exibe o dia em que a transferência de volume foi iniciada.

- **Tempo Final**

Exibe a hora de término da transferência de volume com data.

Informações relacionadas

- Para obter informações sobre a visualização **Relacionamento: MetroCluster**, consulte "[Monitoramento das configurações do MetroCluster](#)".
- Para obter informações sobre a visualização **Relacionamento: Status de transferência do último mês**, consulte "[Relacionamento: Visualização do status de transferência do último mês](#)".
- Para obter informações sobre a visualização **Relacionamento: Todos os relacionamentos**, consulte "[Relacionamento: Visualização da taxa de transferência do último mês](#)".

Gerar relatórios personalizados

Relatórios do Unified Manager

O Active IQ Unified Manager (antigo OnCommand Unified Manager) oferece a capacidade de visualizar, personalizar, baixar e agendar relatórios para seus sistemas de armazenamento ONTAP . Os relatórios podem fornecer detalhes sobre a capacidade, integridade, desempenho, segurança e relacionamentos de proteção do sistema de armazenamento.

A nova funcionalidade de relatórios e agendamento do Unified Manager introduzida no Active IQ Unified Manager 9.6 substitui o mecanismo de relatórios anterior que foi descontinuado na versão 9.5 do Unified Manager.

Os relatórios fornecem diferentes visões da sua rede, oferecendo inteligência acionável 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 visualizações personalizadas para reutilização, baixá-las como relatórios e programá-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 classificações complexas, filtros em camadas, tabelas dinâmicas e gráficos. Quando estiver satisfeito com o relatório do Excel resultante, você pode carregar o arquivo do Excel para uso sempre que o relatório for agendado e compartilhado.

Além de gerar relatórios da interface do usuário, você pode extrair dados de integridade, segurança e desempenho do Unified Manager usando estes métodos adicionais:

- Usando Open Database Connectivity (ODBC) e ferramentas ODBC para acessar diretamente o banco de dados para obter informações do cluster
- Executando APIs REST do Unified Manager para retornar as informações que você está interessado em revisar

A partir desta versão do Active IQ Unified Manager, os seguintes aprimoramentos foram feitos nos relatórios:

- Um e-mail é enviado para um relatório conforme o cronograma configurado. 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, você ainda poderá identificar o nome do host de onde o relatório foi gerado devido a esse aprimoramento.

Pontos de acesso para geração de relatórios

Você pode reunir informações no Unified Manager sobre seus clusters para criar relatórios da interface do usuário, consultas ao banco de dados MySQL e APIs REST.

Estas seções descrevem os relatórios e o agendamento do Unified Manager por meio da interface do usuário.

Há três maneiras de acessar os recursos de relatórios fornecidos pelo Unified Manager:

- Extraindo dados diretamente das páginas de inventário na interface do usuário.

- Usando Open Database Connectivity (ODBC) e ferramentas ODBC para acessar todos os objetos disponíveis.
- Executando APIs REST do Unified Manager para retornar as informações que você deseja revisar.

Estas seções descrevem os relatórios e o agendamento do Unified Manager por meio da interface do usuário.

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 está monitorando. Os dados são persistidos em vários esquemas no banco de dados MySQL.

Todos os dados da tabela dos seguintes bancos de dados estão disponíveis:

Banco de dados	Descrição
modelo netapp	Dados sobre os objetos nos controladores ONTAP .
netapp_model_view	Dados sobre os objetos nos controladores ONTAP , adequados para consumo de ferramentas de relatório.
netapp_desempenho	Contadores de desempenho específicos do cluster.
ocum	Dados e informações do aplicativo Unified Manager para dar suporte à filtragem da interface do usuário, classificação e cálculo de alguns campos derivados.
ocum_report	Dados para configuração de inventário e informações relacionadas à capacidade.
ocum_report_birth	Visualizações para configuração de inventário e dados relacionados à capacidade, adequadas para consumo de ferramentas de relatório.
opm	Definições de configuração de desempenho e informações de limite.
monitor de escala	Dados sobre problemas de desempenho e integridade do aplicativo Unified Manager.
modelo_vmware	Dados de objetos VMware para datastores hospedados no armazenamento NetApp .
visualização_do_modelo_vmware	Visualizações de dados de objetos VMware para datastores hospedados no armazenamento NetApp , adequados para consumo de ferramentas de relatório.

Banco de dados	Descrição
desempenho_vmware	Dados do contador de desempenho do VMware para datastores hospedados no armazenamento NetApp .

Um usuário de relatórios — um usuário de banco de dados com a função Esquema de relatório — pode acessar os dados nessas tabelas. Este usuário tem acesso somente leitura a relatórios e outras visualizações de banco de dados diretamente do banco de dados do Unified Manager. Observe que este usuário não tem permissão para acessar nenhuma tabela que contenha dados do usuário ou informações de credenciais do cluster.

APIs REST do Unified Manager que podem ser usadas para relatórios

Você pode usar APIs REST para ajudar a gerenciar seus 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 interface da Web do Unified Manager, na barra de menus, clique no botão **Ajuda** e selecione **Documentação da API**. Para obter informações sobre APIs REST do Unified Manager, consulte "[Introdução às APIs REST do Active IQ Unified Manager](#)".

Você deve ter a função de Operador, Administrador de Armazenamento ou Administrador de Aplicativo para acessar as APIs REST.

Entenda os 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.

Ao personalizar uma visualização, 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, carregar o arquivo de volta no Unified Manager. Se você agendar um relatório usando essa visualização, ele usará o arquivo Excel que você carregou para criar relatórios robustos que você pode compartilhar.

Você pode gerenciar todos os relatórios que foram agendados na página Agendamentos de Relatórios.



Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento para gerenciar relatórios.

Você pode baixar relatórios como arquivos de valores separados por vírgula (CSV), Excel ou PDF.

Entenda a relação de exibição e relatório

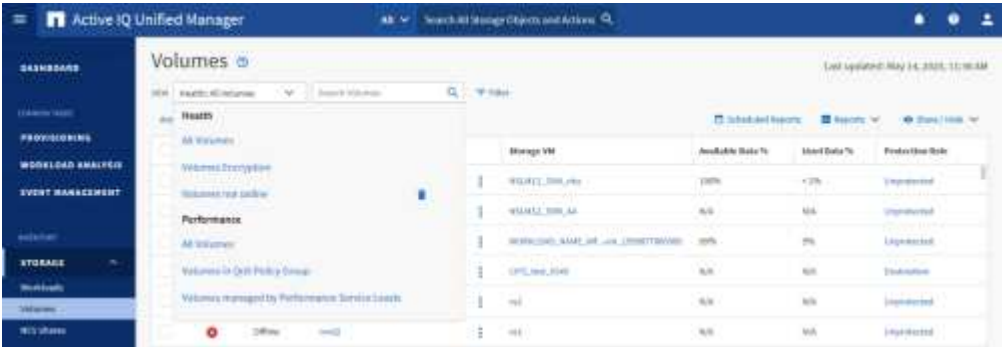
As visualizações e páginas de inventário se tornam relatórios quando você as baixa ou as agenda.

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.

No menu suspenso de exibição, os itens com o ícone de exclusão são exibições personalizadas existentes que você ou outro usuário criou. Itens sem ícone são visualizações padrão fornecidas com o Unified Manager. As visualizações padrão não podem ser modificadas ou excluídas.



- Se você excluir uma exibição personalizada da lista, ela também excluirá todos os arquivos do Excel ou relatórios agendados 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 email, de acordo com o agendamento do relatório. Ao alterar as visualizações, certifique-se de que suas alterações funcionem com quaisquer personalizações associadas do Excel usadas 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.



Somente usuários com a função de Administrador de Aplicativo ou Administrador de Armazenamento podem ver o ícone de exclusão, alterar ou excluir uma exibição ou alterar ou excluir 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 armazenamento ou rede
Capacidade	Aglomerados
	Agregados
	Volumes
	Qtrees

Tipo	Objeto de armazenamento ou rede
Saúde	Aglomerados Nós Agregados VMs de armazenamento Volumes Ações SMB/CIFS Ações NFS
Desempenho	Aglomerados Nós Agregados VMs de armazenamento Volumes LUNs Espaços para nomes NVMe Interfaces de rede (LIFs) Portos
Qualidade de 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 (disponíveis na página Volumes)	Todos os relacionamentos Status de transferência do último mês Taxa de transferência do último mês
Segurança	VMs de armazenamento Aglomerados

Limitações de relatórios

Há algumas limitações na 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 o agendamento e os destinatários de 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:

- crie uma nova visualização e agende um relatório a partir dessa visualização (preferencial)
- passe o mouse sobre o relatório, copie o SQL e extraia 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 quaisquer relatórios personalizados.

Relacionamento entre agendamento e relatório

Você pode criar muitos agendamentos diferentes com qualquer combinação de destinatários para cada relatório salvo. No entanto, você não pode reutilizar o agendamento para vários relatórios.

Proteção de relatórios

Qualquer usuário com as permissões apropriadas pode editar ou excluir relatórios. Não há como impedir que outros usuários removam ou façam alterações em visualizações ou programações salvas.

Relatórios de eventos

Embora você possa personalizar a visualização do evento e baixar o relatório resultante no formato CSV, não é possível agendar relatórios de eventos recorrentes para geração e distribuição.

Anexos de relatórios

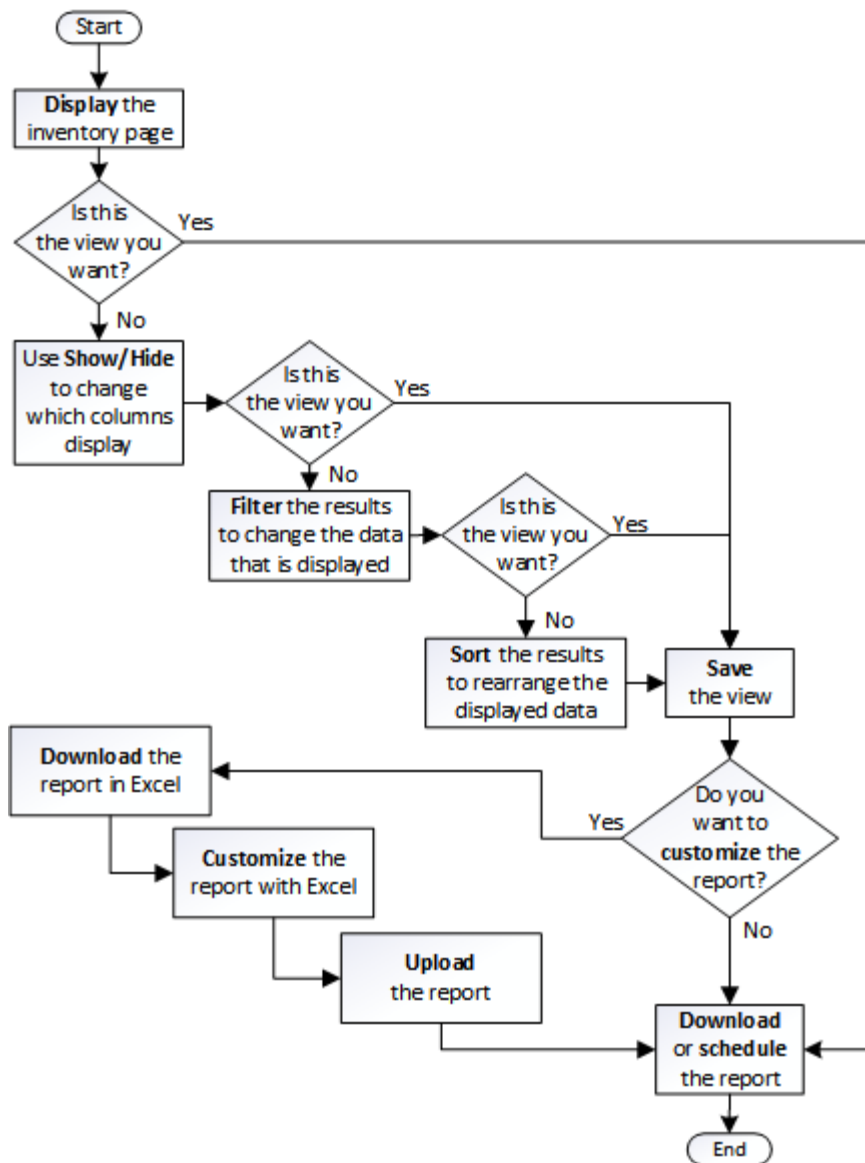
Relatórios não podem ser enviados no corpo de um e-mail. Em vez disso, os relatórios são enviados apenas como anexos em PDF, Excel ou CSV.

Trabalhar com relatórios

Aprenda como encontrar e personalizar visualizações de páginas de inventário em relatórios agendados compartilháveis.

Fluxo de trabalho do relatório

Árvore de decisão que descreve o fluxo de trabalho do relatório.



Início rápido de relatórios

Crie um relatório personalizado de exemplo para experimentar explorar visualizações e agendar relatórios. Este relatório de início rápido encontra uma lista de volumes que você pode querer mover para a camada de nuvem porque há uma quantidade considerável de dados inativos (frios). Você abrirá a visualização Desempenho: Todos os volumes, personalizará a visualização usando filtros e colunas, salvará a visualização personalizada como um relatório e agendará o relatório para ser compartilhado uma vez por semana.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado agregados do FabricPool e ter volumes nesses agregados.

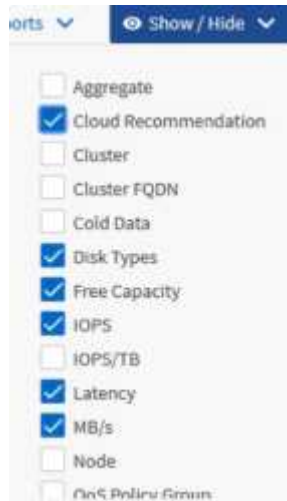
Siga os passos abaixo para:

- Abra a visualização padrão

- Personalize as colunas filtrando e classificando os dados
- Salvar a visualização
- Agende um relatório para ser gerado para a visualização personalizada

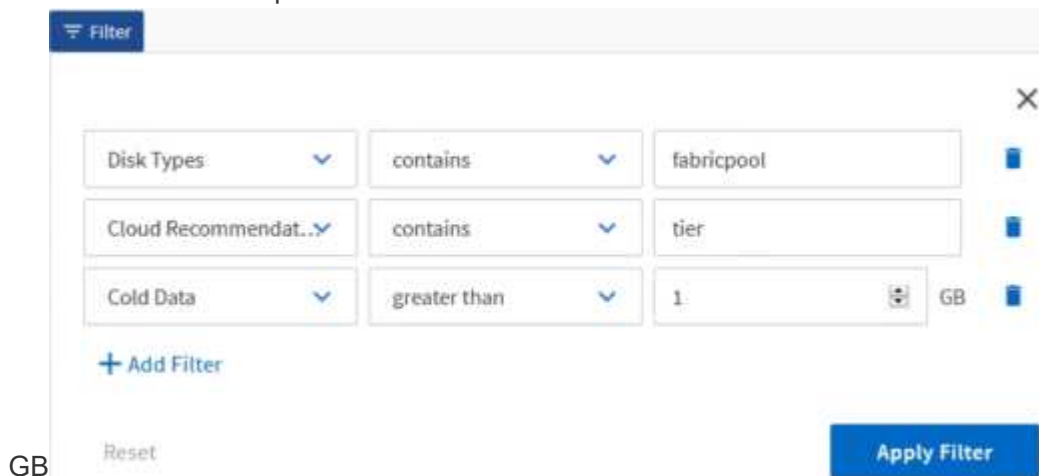
Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Desempenho > Todos os volumes**.
3. Clique em **Mostrar/Ocultar** para garantir que a coluna “Tipos de disco” apareça na exibição.



Adicione ou remova outras colunas para criar uma exibição que contenha os campos importantes para o seu relatório.

4. Arraste a coluna “Tipos de disco” para perto da coluna “Recomendação de nuvem”.
5. Clique no ícone de filtro para adicionar os três filtros a seguir e, em seguida, clique em **Aplicar filtro**:
 - Tipos de disco contém FabricPool
 - Recomendação de nuvem contém nível
 - Dados frios maiores que 10



Observe que cada filtro é unido por um AND lógico para que todos os volumes retornados atendam a todos os critérios. Você pode adicionar no máximo cinco filtros.

6. Clique na parte superior da coluna Dados Frios para classificar os resultados de modo que os volumes com mais dados frios apareçam na parte superior da visualização.
7. Quando a exibição é personalizada, o nome da exibição é Exibição não salva. Nomeie a exibição para refletir o que ela está mostrando, por exemplo, "Vols alteram política de níveis". Quando terminar, clique na marca de seleção ou pressione **Enter** para salvar a visualização 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

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagntsdzt	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

8. Baixe o relatório como um arquivo **CSV**, **Excel** ou **PDF** para ver o resultado antes de agendá-lo ou compartilhá-lo.

Abra o arquivo com um aplicativo instalado, como o Microsoft Excel (CSV ou Excel) ou o Adobe Acrobat (PDF), ou salve o arquivo.



Você pode personalizar ainda mais seu relatório usando filtros complexos, classificações, tabelas dinâmicas ou gráficos baixando a visualização como um arquivo Excel. Depois de abrir o arquivo no Excel, use os recursos avançados para personalizar seu relatório. Quando estiver satisfeito, carregue o arquivo Excel. Este arquivo, com suas personalizações, é aplicado à exibição quando o relatório é executado.

Para obter mais informações sobre como personalizar relatórios usando o Excel, consulte *Exemplos de relatórios do Microsoft Excel*.

9. Clique no botão **Relatórios agendados** na página de inventário. Todos os relatórios agendados 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

Schedule Name	View	Recipients	Frequency	Format
Weekly / Vols c... tiering policy	Performance / V... tiering policy	user@company.com	Weekly - Monday 1:00 PM	CSV

10. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios para que você possa definir as características do agendamento para o novo relatório.
11. Digite um nome para o 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

O seguinte relatório de exemplo está no formato CSV:

Status	Volume	Volume Id	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	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 exemplo 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	99018	aggr5_vs
Ok	nfs_vol4	Snapshot	379.64	2676.57	3072	ocum-mo	99113	aggr4

Com base nos resultados mostrados no relatório, talvez você queira usar o ONTAP System Manager ou o ONTAP CLI para alterar a política de camadas para “auto” ou “all” para determinados volumes para descarregar mais dados frios para a camada de nuvem.

Pesquisar um relatório agendado

Você pode pesquisar relatórios agendados por nome, nome da exibição, tipo de objeto ou destinatários.

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Agendamentos de relatórios**.
2. Use o campo de texto **Pesquisar relatórios agendados**.

Para encontrar relatórios de ...	Tentar ...
Nome do cronograma	Digite parte do nome do agendamento do relatório.
Ver nome	Digite parte do nome da exibição do relatório. As visualizações padrão e personalizadas aparecem na lista de visualizações.
Destinatário	Digite parte do endereço de e-mail.
Tipo de arquivo	Digite "PDF", "CSV" ou "XLSX".

3. Você pode clicar em um título de 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 visualizações para que você possa criar um relatório que contenha todas as informações necessárias para gerenciar seus clusters ONTAP .

Comece com uma página de inventário padrão ou uma visualização personalizada e, em seguida, personalize-a adicionando ou removendo colunas, alterando a ordem das colunas, filtrando os dados ou classificando uma coluna específica em ordem crescente ou decrescente.

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 arquivo Excel personalizado. Se você agendar um relatório usando essa visualização, 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*.



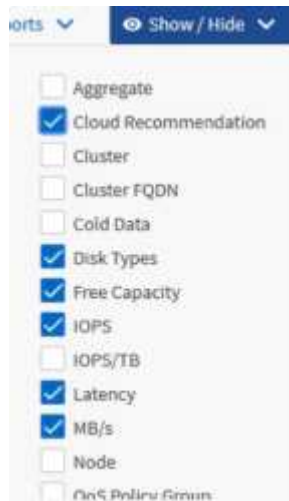
Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento para gerenciar relatórios.

Personalizar colunas

Use **Mostrar/Ocultar** para escolher as colunas que deseja usar no seu 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 as colunas para reorganizá-las na ordem desejada no seu relatório.
3. Nomeie a exibição não salva para salvar suas alterações.

Filtrar dados

Filtre os dados para garantir que os resultados correspondam aos requisitos do seu relatório. A filtragem permite que você exiba apenas os dados nos quais está interessado.

Passos

1. Clique no ícone de filtro para adicionar filtros para focar os resultados que você deseja visualizar e, em seguida, clique em **Aplicar filtro**.

The screenshot shows a filter configuration window. At the top is a 'Filter' button with a dropdown arrow. Below it is a table of filter rules:

Disk Types	contains	fabricpool	
Cloud Recommendation	contains	tier	
Cold Data	greater than	1	GB

Below the table is a '+ Add Filter' button. At the bottom left is a 'Reset' button, and at the bottom right is a blue 'Apply Filter' button. A close 'X' button is in the top right corner.

2. Nomeie a exibição não salva para salvar suas alterações.

Classificar dados

Para classificar os resultados, clique em uma coluna e indique a ordem crescente ou decrescente. A classificação de dados prioriza as informações necessárias para o relatório.

Passos

1. Clique na parte superior de uma coluna para classificar os resultados de modo que as informações mais importantes apareçam no topo da visualização.
2. Nomeie a exibição não salva para salvar suas alterações.

Usando a pesquisa para refinar sua visualização

Depois de obter 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 a exibição personalizada ou padrão que você deseja usar como base para seu relatório.
2. Digite no campo Pesquisar para refinar os dados listados na exibição. Você pode inserir dados parciais em qualquer uma das colunas exibidas. Por exemplo, se você quiser pesquisar nós que incluam "US_East" no nome, você pode refinar a lista completa de nós.

Os resultados da sua pesquisa são salvos na visualização personalizada e usados no relatório agendado resultante.

3. Nomeie a exibição não salva para salvar suas alterações.

Use o Excel para personalizar seu relatório

Depois de salvar a visualização, você pode baixá-la no formato de pasta de trabalho do Excel (.xlsx). Ao abrir o arquivo do Excel, você pode usar recursos avançados do Excel para personalizar seu relatório.

Antes de começar

Você só pode carregar um arquivo de pasta de trabalho do Excel com a extensão .xlsx.

Por exemplo, alguns recursos avançados do Excel que você pode usar em seu relatório incluem:

- Classificação de várias colunas
- Filtragem complexa
- Tabelas dinâmicas
- Gráficos



- O arquivo Excel baixado usa o nome de arquivo padrão para a exibição, não o nome salvo.
 - O formato é <View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx.
 - Por exemplo, uma visualização salva personalizada chamada Volumes-not online tem um nome de arquivo de health-volumes-05-May-2020-19-18-00.xlsx se salvo naquele dia e hora.
- Você pode adicionar planilhas ao arquivo do Excel, mas não alterar as planilhas existentes.
 - Não altere as planilhas, 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 “dados”. Use as fórmulas da página de dados para criar gráficos em novas páginas.
 - Não nomeie uma nova planilha com dados ou informações.
- Se existir um arquivo Excel personalizado, haverá uma marca de seleção 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 a exibição padrão, personalizada ou salva que você deseja usar como base para seu relatório.
2. Selecione **Relatórios > Baixar Excel**.
3. Salve o arquivo. O arquivo é salvo na sua pasta de downloads.
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 no local original usando o nome do arquivo original antes de enviá-lo.
5. Personalize o arquivo usando recursos do Excel, como classificações complexas, 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 arquivo que você modificou. O arquivo baixado

mais recentemente é carregado do mesmo local de arquivo.

7. Envie para você mesmo um relatório de teste usando o recurso **Relatórios agendados**.

Baixar relatórios

Você pode baixar relatórios e salvar os dados em uma unidade local ou de rede como um arquivo de valores separados por vírgula (CSV), 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 baixar o relatório como um dos seguintes:

Escolher	Para...
Baixar CSV	Salve o relatório como um arquivo de valores separados por vírgula (CSV).
Baixar PDF	Salve o relatório como um arquivo .pdf.
Baixar 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 agendá-la usando o Active IQ Unified Manager. Você pode gerenciar relatórios agendados, alterando 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. As exceções são eventos, que são relatórios que você pode baixar como arquivos CSV, mas 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 classificações complexas, filtros em camadas, tabelas dinâmicas e gráficos. Quando estiver satisfeito com o relatório do Excel resultante, você pode carregar o arquivo do Excel para uso sempre que o relatório for agendado e compartilhado.

Você pode agendar as visualizações integradas ou as visualizações que você personalizar. Você pode escolher qual tipo de arquivo enviar: CSV, PDF ou XSLX. Ao agendar um relatório pela primeira vez, você pode baixá-lo e se definir como o único destinatário a vê-lo, assim como seus destinatários o verão.

Agendar um relatório

Depois de ter uma exibição ou arquivo Excel que você deseja agendar para geração e distribuição regulares, você pode agendar o relatório.

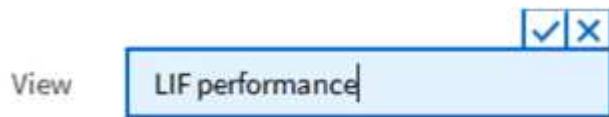
Antes de começar

- Você deve ter a função de Administrador de Aplicativos 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 do Unified Manager.
- O servidor de e-mail deve ser configurado para permitir o envio de anexos com os e-mails gerados.

Use as etapas a seguir para testar e agendar a geração de um relatório para uma exibição. Selecione ou personalize a visualização que deseja usar. O procedimento a seguir usa uma visualização de rede que mostra o desempenho das suas interfaces de rede, mas você pode usar qualquer visualização que desejar.

Passos

1. Abra sua visualização. Este exemplo usa a exibição de rede padrão que mostra o desempenho do LIF. No painel de navegação esquerdo, clique em **Rede > Interfaces de rede**.
2. Personalize a visualização conforme necessário usando os recursos integrados do Unified Manager.
3. Depois de personalizar a visualização, você pode fornecer um nome exclusivo no campo **Visualização** e clicar na marca de seleção para salvá-lo.



4. Você pode usar os recursos avançados do Microsoft® Excel para personalizar seu relatório. Para mais detalhes, veja "[Usando o Excel para personalizar seu relatório](#)".
5. Para ver a saída antes de agendá-la ou compartilhá-la:

Opção	Descrição
Se você usou o Excel para personalizar o relatório	Visualize o arquivo Excel baixado existente.
Se você não usou o Excel para personalizar o relatório	Baixe o relatório como um arquivo CSV , PDF ou XLSX .

Abra o arquivo com um aplicativo instalado, como o Microsoft Excel (CSV/XSLX) ou o Adobe Acrobat (PDF).

6. Se estiver satisfeito com o relatório, clique em **Relatórios agendados**.
7. Na página Cronogramas de relatórios, clique em **Adicionar cronograma**.
8. Aceite o nome padrão, que é uma combinação do nome da exibição 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 de todos os destinatários do relatório.
10. Especifique com que frequência o relatório será gerado e enviado aos destinatários. Você pode escolher **Diário**, **Semanal** ou **Mensal**.
11. Selecione o formato, **PDF**, **CSV** ou **XSLX**.



Para relatórios em que você usou o Excel para personalizar o conteúdo, sempre selecione **XSLX**.

12. Clique na marca de seleção (✓) para salvar o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência agendada.

Agendar relatórios .rptdesign importados

Você pode agendar relatórios existentes que foram criados e importados em uma versão anterior do Unified Manager.

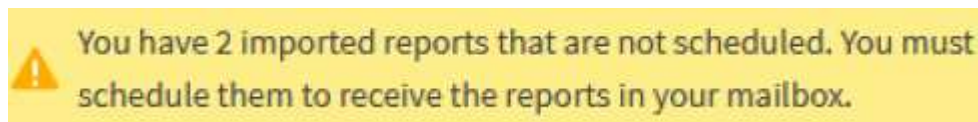
O agendamento de relatórios importados requer o seguinte:

- relatórios de arquivo .rptdesign projetados pelo BIRT importados em uma versão anterior do Unified Manager
- aplicável ao atualizar para o Unified Manager 9.6 GA ou posterior

Após a atualização para o Unified Manager 9.6 GA ou posterior, a página Agendamentos de relatórios lista os relatórios importados. Você pode editar o agendamento desses relatórios para especificar os endereços de e-mail dos destinatários, a frequência e o formato (PDF ou CSV). Caso contrário, esses relatórios não poderão ser editados ou visualizados na interface do usuário do Unified Manager.

Passos

1. Abra a página Agendamentos de relatórios. Se você tiver importado relatórios, uma mensagem será exibida.



2. Clique no nome **Exibir** 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 no ícone mais .

Gerenciar agendamentos de relatórios

Você pode gerenciar seus agendamentos de relatórios na página Agendamentos de Relatórios. Você pode visualizar, modificar ou excluir programações existentes.



Antes de começar

Não é possível agendar novos relatórios na página Agendamentos de Relatórios. Você só pode adicionar relatórios agendados das páginas de inventário de objetos.

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Agendamentos de relatórios**.
2. Na página Cronogramas de Relatórios:

Se você quiser...	Então...
Ver uma programação existente	Percorra a lista de relatórios existentes usando as barras de rolagem e os controles de página.

Se você quiser...	Então...
Editar uma programação existente	- Clique no ícone mais  para o cronograma que você deseja usar. - Clique em Editar. - Faça as alterações necessárias. - Clique na marca de seleção para salvar suas alterações.
Excluir uma programação existente	- Clique no ícone mais  para o cronograma que você deseja usar. - Clique em Excluir. - Confirme sua decisão.

Editar relatórios agendados

Depois que os relatórios forem agendados, você poderá editá-los na página Agendamentos de Relatórios.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

- No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Agendamentos 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	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



Se você tiver as permissões apropriadas, poderá alterar qualquer relatório e sua programação no sistema.

- Clique no ícone mais  para o cronograma que você deseja alterar.
- Clique em **Editar**.
- Você pode alterar o **Nome do agendamento**, a lista de **Destinatários**, a **Frequência** e o **Formato** do agendamento do relatório.

5. Quando terminar, clique na marca de seleção para salvar suas alterações.

Excluir relatórios agendados

Depois que os relatórios forem agendados, você poderá excluí-los da página Agendamentos de Relatórios.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento > Agendamentos 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	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	⋮
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	⋮
Weekly / LIF performance	Performance / LIF performance	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 **⋮** para o cronograma que você deseja remover.
3. Clique em **Excluir**.
4. Confirme sua decisão.

O relatório agendado será 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 agendados que usam essa exibição também serão excluídos.

Relatórios personalizados de amostra

Esses relatórios personalizados de exemplo são comumente usados para ajudar você a identificar problemas potenciais e responder a eles antes que eles ocorram.

A lista de relatórios nesta seção não é exaustiva e aumentará com o tempo. Você pode sugerir relatórios personalizados para adicionar a esta seção fornecendo feedback sobre a documentação.



Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento para gerenciar relatórios.

Personalizar relatórios de armazenamento em cluster

Os relatórios de exemplo de armazenamento em cluster nesta seção são apenas exemplos para ajudar você a entender como criar relatórios sobre a capacidade do cluster para ajudar a monitorar os recursos do seu sistema de armazenamento.

Crie um relatório para visualizar a capacidade por modelo de cluster

Você pode criar um relatório para analisar a capacidade de armazenamento e a utilização de clusters com base no modelo do sistema de armazenamento.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada que exiba a capacidade por modelo de cluster e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Clusters**.
2. No menu Exibir, selecione **Capacidade > Todos os clusters**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas, como “Cluster FQDN” e “Versão do SO”, que você não deseja no relatório.
4. Arraste a **Capacidade Bruta Total**, o **Modelo/Família** e as três colunas agregadas para perto da coluna **Cluster**.
5. Clique na parte superior da coluna “Modelo/Família” para classificar os resultados por tipo de cluster.
6. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo, “Capacidade por Modelo de Cluster”.
7. Clique no botão **Relatórios agendados** na página de inventário.
8. Clique em **Adicionar agendamento** para adicionar uma nova linha à página **Agendamentos de relatórios** para que você possa definir as características do agendamento para o novo relatório.
9. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira adicionar mais capacidade a determinados clusters ou atualizar modelos de cluster mais antigos.

Crie um relatório para identificar clusters com maior capacidade de LUN não alocada

Você pode criar um relatório para encontrar os clusters com maior capacidade de LUN não alocada, maior que 0,5 TB, para ajudar a identificar onde você pode adicionar cargas de trabalho adicionais.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada que exiba clusters com a maior capacidade de LUN não alocada e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Clusters**.
2. No menu Exibir, selecione **Capacidade > Todos os clusters**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Arraste a coluna “Capacidade de LUN não alocada” para perto da coluna “Par de HA”.
5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Aplicar filtro**:
 - Capacidade de LUN não alocada maior que 0,5 TB
6. Clique na parte superior da coluna “Capacidade de LUN não alocada” para classificar os resultados pela maior quantidade de capacidade de LUN não alocada.
7. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo “Capacidade de LUN mais não alocada” e clique na marca de seleção (✓).
8. Clique no botão **Relatórios agendados** na página de inventário.
9. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios para que você possa definir as características do agendamento para o novo relatório.
10. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos 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.

Crie um relatório para visualizar pares de HA com maior capacidade disponível

Você pode criar um relatório para encontrar os pares de alta disponibilidade (HA) com maior capacidade de provisionar novos volumes e LUNs.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada que exiba pares de HA classificados pela maior capacidade disponível para provisionar novos volumes e LUNs e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Clusters**.
2. No menu Exibir, selecione **Capacidade > Todos os clusters**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Arraste a coluna “Capacidade agregada não utilizada” para perto da coluna “Par HA”.

5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Aplicar filtro**:
 - Capacidade agregada não utilizada maior que 0,5 TB
6. Clique na parte superior da coluna “Capacidade agregada não utilizada” para classificar os resultados pela maior quantidade de capacidade agregada não utilizada.
7. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo, “Capacidade agregada menos utilizada”, e clique na marca de seleção (✓).
8. Clique no botão **Relatórios agendados** na página de inventário.
9. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios para que você possa definir as características do agendamento para o novo relatório.
10. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira balancear os pares de HA com base na capacidade agregada.

Crie um relatório para visualizar nós executando versões mais antigas do ONTAP

Você pode criar um relatório para exibir a versão do software ONTAP instalada em todos os nós do cluster para que você possa ver quais nós devem ser atualizados.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos 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, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Nós**.
2. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
3. Arraste a coluna “Versão do SO” para perto da coluna “Nó”.
4. Clique no topo da coluna “Versão do SO” para classificar os resultados pela versão mais antiga do ONTAP.
5. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo, “Nós por versão ONTAP”.
6. Clique no botão **Relatórios agendados** na página de inventário.
7. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios para que você possa definir as características do agendamento para o novo relatório.
8. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira atualizar os nós que executam versões

mais antigas do ONTAP.

Personalizar relatórios de capacidade agregada

Esses relatórios personalizados de amostra são usados para ajudar você a identificar e responder a possíveis problemas relacionados à capacidade de armazenamento agregada.

Os relatórios nesta seção são apenas exemplos para ajudar você a entender como criar relatórios sobre capacidade agregada para ajudar você a monitorar os recursos do seu sistema de armazenamento.

Crie um relatório para visualizar os agregados atingindo a capacidade máxima

Você pode criar um relatório para encontrar os agregados que estão atingindo a capacidade máxima para que você possa adicionar mais capacidade ou mover cargas de trabalho para outros agregados.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada que exiba os agregados atingindo a capacidade máxima e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Agregados**.
2. No menu Exibir, selecione **Capacidade > Todos os agregados**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Aplicar filtro**:
 - Dias para completar menos de 45 dias
5. Clique na parte superior da coluna “Dias para atingir a capacidade máxima” para classificar os resultados pelo menor número de dias restantes para atingir a capacidade máxima.
6. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo, “Dias até a capacidade agregada total”, e clique na marca de seleção (✓).
7. Clique no botão **Relatórios agendados** na página de inventário.
8. Clique em **Adicionar agendamento** para adicionar uma nova linha à página **Agendamentos de relatórios** para que você possa definir as características do agendamento para o novo relatório.
9. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira aumentar o armazenamento em agregados atingindo a capacidade máxima. Além disso, talvez você queira aumentar o limite de Dias até a capacidade máxima para mais do que o padrão de 7 dias, para receber eventos que forneçam mais tempo para reagir quando o espaço estiver ficando baixo em agregados.

Crie um relatório para visualizar agregados que estão 80% ou mais cheios

Você pode criar um relatório para destacar os agregados que estão 80% ou mais cheios.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada que exiba agregados que estejam 80% ou mais cheios e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Agregados**.
2. No menu Exibir, selecione **Capacidade > Todos os agregados**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Arraste as colunas "Dados disponíveis %" e "Dados usados %" para perto da coluna "Agregado".
5. Clique no ícone de filtro, adicione os seguintes filtros e clique em **Aplicar filtro**:
 - Dados usados % é maior que 80%
6. Clique na parte superior da coluna "Dados usados %" para classificar os resultados por porcentagem de capacidade.
7. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo, "Agregados quase cheios", e clique na marca de seleção (✓).
8. Clique no botão **Relatórios agendados** na página de inventário.
9. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios para que você possa definir as características do agendamento para o novo relatório.
10. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira mover alguns dados de determinados agregados.

Crie um relatório para visualizar agregados que estão supercomprometidos

Você pode criar um relatório para analisar a capacidade de armazenamento e o uso de agregados, além de visualizar agregados que estão supercomprometidos.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada que exiba agregados que excedem o limite de comprometimento excessivo e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Agregados**.
2. No menu Exibir, selecione **Capacidade > Todos os agregados**.

3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Arraste a coluna “Capacidade supercomprometida %” para perto da coluna “Agregado”.
5. Clique no ícone de filtro, adicione os seguintes filtros e clique em **Aplicar filtro**:
 - Capacidade supercomprometida % é maior que 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 supercomprometidos”, e clique na marca de seleção (✓).
8. Clique no botão **Relatórios agendados** na página de inventário.
9. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios para que você possa definir as características do agendamento para o novo relatório.
10. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira adicionar mais capacidade aos agregados ou mover alguns dados de determinados agregados.

Personalizar relatórios de capacidade de volume

Esses relatórios personalizados de amostra são usados para ajudar você a identificar e responder a possíveis problemas relacionados à capacidade de volume e ao desempenho.

Crie um relatório para identificar volumes próximos da capacidade máxima que tenham a Exclusão Automática de Snapshot desativada

Você pode criar um relatório que contém a lista de volumes que estão se aproximando da capacidade máxima com o recurso de exclusão automática de instantâneo desabilitado. Os resultados podem ajudar a identificar volumes nos quais você pode querer configurar a exclusão automática de instantâneos.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Siga as etapas abaixo para criar uma exibição personalizada que exiba as colunas necessárias na ordem correta e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Capacidade > Todos os volumes**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Arraste e solte as colunas “Exclusão automática de instantâneo” e “Dias para o máximo” perto da coluna “Capacidade de dados disponível”.

5. Clique no ícone de filtro, adicione os dois filtros a seguir e clique em **Aplicar filtro**:
 - Dias para completar menos de 30 dias
 - A exclusão automática de instantâneos está desabilitada
6. Clique no topo da coluna **Dias para completar** para que os volumes com menos dias restantes apareçam no topo da lista.
7. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo “Volumes próximos da capacidade”.
8. Clique no botão **Relatórios agendados** na página de inventário.
9. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira habilitar a exclusão automática de instantâneos nos volumes ou encontrar uma maneira de aumentar o espaço disponível.

Crie um relatório para identificar o espaço usado por volumes com provisionamento fino desabilitado

Quando um volume não é provisionado finamente, ele ocupa todo o espaço no disco, conforme definido quando o volume foi criado. Identificar volumes que têm o provisionamento fino desabilitado ajuda você a decidir se deseja habilitar o provisionamento fino em determinados volumes.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Siga as etapas abaixo para criar uma exibição personalizada que exiba as colunas necessárias na ordem correta e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Capacidade > Todos os volumes**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Arraste e solte as colunas “Dados usados %” e “Thin Provisioned” perto da coluna “Capacidade de dados disponível”.
5. Clique no ícone de filtro, adicione o seguinte filtro, **Thin provisioned é Não**, e então clique em **Aplicar filtro**.
6. Clique na parte superior da coluna “Dados usados %” para classificar os resultados de modo que os volumes com a maior porcentagem apareçam no topo da lista.
7. Salve a visualização com um nome que reflita o que a visualização está mostrando, por exemplo “Vols no thin provisioning”.
8. Clique no botão **Relatórios agendados** na página de inventário.
9. Clique em **Adicionar agendamento** para adicionar uma nova linha à página **Agendamentos de relatórios** para que você possa definir as características do agendamento para o novo relatório.
10. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira habilitar o provisionamento fino em determinados volumes.

Crie um relatório para identificar volumes em agregados do FabricPool que devem mover dados para a camada de nuvem

Você pode criar um relatório que contém a lista de volumes que atualmente residem em agregados do FabricPool, que têm uma recomendação de nuvem de Nível e que têm uma grande quantidade de dados inativos. Este relatório pode ajudar você a decidir se deve alterar a política de camadas para determinados volumes para “automático” ou “todos” para descarregar mais dados frios (inativos) para a camada de nuvem.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado agregados do FabricPool 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, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Desempenho > Todos os volumes**.
3. No seletor de colunas, certifique-se de que a coluna “Tipo de disco” apareça na exibição.

Adicione ou remova outras colunas para criar uma visualização importante para seu relatório.

4. Arraste e solte a coluna “Tipo de disco” perto da coluna “Recomendação de nuvem”.
5. Clique no ícone de filtro, adicione os três filtros a seguir e clique em **Aplicar filtro**:
 - O tipo de disco contém FabricPool
 - Recomendação de nuvem contém nível
 - Dados frios maiores que 10 GB

Filter configuration dialog box showing three filter rules:

- Disk Types: contains fabricpool
- Cloud Recommendation: contains tier
- Cold Data: greater than 10 GB

Buttons: + Add Filter, Reset, Cancel, Apply Filter

6. Clique na parte superior da coluna Dados Frios para que os volumes com mais dados frios apareçam no topo da visualização.
7. Salve a exibição com um nome que reflita o que a exibição está mostrando, por exemplo “Vols alteram política de níveis”.

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 3

Assign Performance Threshold Policy		Clear Performance Threshold Policy		Schedule Report		
Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_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

8. Clique no botão **Relatórios agendados** na página de inventário.
9. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios para que você possa definir as características do agendamento para o novo relatório.
10. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira usar o System Manager ou o ONTAP CLI para alterar a política de camadas para “auto” ou “all” para determinados volumes para descarregar mais dados frios para a camada de nuvem.

Personalize relatórios de capacidade do Qtree

Esses relatórios personalizados de amostra são usados para ajudar você a identificar e

responder a possíveis problemas relacionados à capacidade do Qtree.

Crie 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 cheias.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada que exiba qtrees quase cheias e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Qtrees**.
2. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
3. Arraste a coluna “Disco Usado %” para perto da coluna “Qtrees”.
4. Clique no ícone de filtro, adicione os seguintes filtros e clique em **Aplicar filtro**:
 - A porcentagem de disco usado é maior que 75%
5. Clique na parte superior da coluna “Disco usado %” para classificar os resultados por porcentagem de capacidade.
6. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo, “Qtrees quase cheio”, e clique na marca de seleção (✓).
7. Clique no botão **Relatórios agendados** na página de inventário.
8. Clique em **Adicionar agendamento** para adicionar uma nova linha à página **Agendamentos de relatórios** para que você possa definir as características do agendamento para o novo relatório.
9. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira ajustar os limites rígidos e flexíveis do disco (se definidos) ou balancear os dados entre as qtrees.

Personalizar relatórios de compartilhamento NFS

Você pode personalizar relatórios de compartilhamento NFS para analisar informações sobre políticas e regras de exportação NFS para volumes em seus sistemas de armazenamento. Por exemplo, você pode personalizar relatórios para exibir volumes com caminhos de montagem inacessíveis e volumes com a política de exportação padrão.

Crie um relatório para visualizar volumes que tenham um caminho de montagem inacessível

Você pode criar um relatório para encontrar volumes que tenham um caminho de montagem inacessível.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada para volumes que tenham um caminho de montagem inacessível e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Compartilhamentos NFS**.
2. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
3. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Aplicar filtro**:
 - Mount Path Active é Não
4. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo “Volumes com um caminho de montagem inacessível” e clique na marca de seleção (✓).
5. Clique no botão **Relatórios agendados** na página de inventário.
6. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios para que você possa definir as características do agendamento para o novo relatório.
7. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira corrigir os caminhos de montagem inacessíveis.

Crie um relatório para visualizar volumes que estão usando a política de exportação padrão

Você pode criar um relatório para encontrar volumes que estão usando a política de exportação padrão.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada para volumes que estão usando a política de exportação padrão e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Compartilhamentos NFS**.
2. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
3. Arraste a coluna “Política de Exportação” para perto da coluna “Volume”.
4. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Aplicar filtro**:
 - A política de exportação contém padrões
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 agendados** na página de inventário.
7. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios

para que você possa definir as características do agendamento para o novo relatório.

8. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira configurar uma política de exportação personalizada.

Personalizar relatórios de VM de armazenamento

Você pode criar relatórios de VM de armazenamento para analisar informações de volume e visualizar a integridade geral e a disponibilidade de armazenamento. Por exemplo, você pode criar relatórios para exibir SVMs atingindo a contagem máxima de volume e analisar SVMs interrompidos.

Crie um relatório para visualizar as VMs de armazenamento atingindo o limite máximo de volume

Você pode criar um relatório para encontrar SVMs que estão atingindo o limite máximo de volume.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use 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 para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > VMs de armazenamento**.
2. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
3. Arraste as colunas "Contagem de volumes" e "Volumes máximos permitidos" para perto da coluna "VM de armazenamento".
4. Clique na parte superior da coluna "Volumes máximos permitidos" para classificar os resultados pelo maior número de volumes.
5. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo "SVMs atingindo volumes máximos" e clique na marca de seleção (✓).
6. Clique no botão **Relatórios agendados** na página de inventário.
7. Clique em **Adicionar agendamento** para adicionar uma nova linha à página **Agendamentos de relatórios** para que você possa definir as características do agendamento para o novo relatório.
8. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira balancear os volumes atribuídos às VMs de armazenamento ou, se possível, usar o ONTAP System Manager para alterar os volumes máximos

permitidos.

Crie um relatório para visualizar VMs de armazenamento paradas

Você pode criar um relatório para exibir uma lista de todos os SVMs interrompidos.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos 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 para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > VMs de armazenamento**.
2. No menu Exibir, selecione **Saúde > Todas as VMs de armazenamento**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Arraste a coluna "Estado" para perto da coluna "VM de armazenamento".
5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Aplicar filtro**:
 - O estado está parado
6. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo "SVMs interrompidos" e clique na marca de seleção (✓).
7. Clique no botão **Relatórios agendados** na página de inventário.
8. Clique em **Adicionar agendamento** para adicionar uma nova linha à página **Agendamentos de relatórios** para que você possa definir as características do agendamento para o novo relatório.
9. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira investigar por que o SVM foi interrompido para ver se deve reiniciá-los.

Personalizar relatórios de relacionamento de volume

O relatório Inventário de relacionamentos de volume permite que você analise os detalhes do inventário de armazenamento em um cluster, entenda o grau de proteção necessário para os volumes e filtre os detalhes do volume com base na origem da falha, no padrão e nas programações.

Crie um relatório para agrupar relacionamentos de volume por fonte de falha

Você pode criar um relatório que agrupa volumes pelo motivo pelo qual o relacionamento está em um estado não íntegro.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada que agrupa volumes por origem de falha e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Relacionamento > Todos os Relacionamentos**.
3. Selecione **Mostrar/Ocultar** para garantir que as colunas “Saúde do Relacionamento” e “Motivo Não Saudável” apareçam na exibição.

Adicione ou remova outras colunas para criar uma visualização importante para seu relatório.

4. Arraste as colunas “Saúde do Relacionamento” e “Motivo Não Saudável” para perto da coluna “Estado”.
5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Aplicar filtro**:
 - A saúde do relacionamento é ruim
6. Clique na parte superior da coluna “Motivo não saudável” para agrupar os relacionamentos de volume por fonte de falha.
7. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, “Relacionamentos de volume por falha”.
8. Clique no botão **Relatórios agendados** na página de inventário.
9. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode investigar a origem e o impacto de cada tipo de falha.

Crie um relatório para agrupar relacionamentos de volume por problema

Você pode criar um relatório que agrupe relacionamentos de volume por problema.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada que agrupa relacionamentos de volume por problema e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Relacionamento > Todos os Relacionamentos**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Arraste a coluna “Motivo não saudável” para perto da coluna “Estado”.
5. Clique no topo da coluna “Motivo não saudável” para agrupar os volumes por edição.
6. Salve a exibição com um nome específico que reflita o que a exibição está mostrando, por exemplo, “Relacionamentos de volume por problema”.
7. Clique no botão **Relatórios agendados** na página de inventário.

8. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode investigar a origem e o impacto de cada tipo de problema.

Crie um relatório para visualizar tendências de transferência de volume em intervalos de tempo específicos

Você pode criar um relatório que exiba tendências de transferência de volume em intervalos de tempo específicos.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada para volumes em intervalos de tempo específicos e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Relacionamento > Status de transferência do último mês**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Arraste a coluna Duração da transferência para perto da coluna “Resultado operacional”.
5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Aplicar filtro**:
 - Hora de término 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 visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo “Volumes por duração”.
8. Clique no botão **Relatórios agendados** na página de inventário.
9. Digite um nome para o agendamento do relatório, defina a frequência como **Semanal** e preencha os outros campos do relatório. Em seguida, clique na marca de seleção (✓) no final da linha.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode investigar os intervalos de tempo de transferência.

Crie um relatório para visualizar a transferência de volume com falha ou bem-sucedida

Você pode criar um relatório que exiba o status das transferências de volume. Você pode visualizar transferências de volume com e sem sucesso neste relatório.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos 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, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Relacionamento > Status de transferência do último mês**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não deseja no relatório.
4. Arraste a coluna “Resultado da Operação” para perto da coluna “Estado”.
5. Clique na parte superior da coluna “Resultado da operação” para classificar os volumes por status.
6. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo “Volumes por status de transferência”.
7. Clique no botão **Relatórios agendados** na página de inventário.
8. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode investigar o status da transferência.

Crie um relatório para visualizar transferências de volume com base no tamanho da transferência

Você pode criar um relatório para visualizar transferências de volume com base no tamanho da transferência.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada para transferências de volume com base no tamanho da transferência e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Relacionamento > Taxa de transferência do último mês**.
3. Clique na parte superior da coluna “Tamanho total da transferência” para classificar as transferências de volume por tamanho.
4. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo “Volumes por tamanho de transferência”.
5. Clique no botão **Relatórios agendados** na página de inventário.
6. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode investigar os relacionamentos de volume por tamanho de transferência.

Crie um relatório para visualizar as transferências de volume agrupadas por dia

Você pode criar um relatório para visualizar transferências de volume agrupadas por dia.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as etapas a seguir para criar uma exibição personalizada para transferências de volume agrupadas por dia e, em seguida, agende um relatório para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. No menu Exibir, selecione **Relacionamento > Taxa de transferência do último mês**.
3. Clique na parte superior da coluna “Dia” para classificar as transferências de volume por dia.
4. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo “Transferências de volume por dia”.
5. Clique no botão **Relatórios agendados** na página de inventário.
6. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode investigar o volume de transferências por dia.

Personalizar relatórios de desempenho de volume

Esses relatórios personalizados de amostra são usados para ajudar você a identificar e responder a possíveis problemas relacionados ao desempenho do volume.

Crie um relatório para visualizar volumes com uma grande quantidade de dados inativos em um agregado que não seja habilitado para FabricPool

Você pode criar um relatório para exibir volumes com uma grande quantidade de dados inativos em um agregado não FabricPool . Isso pode ajudar você a identificar volumes que devem ser movidos para um agregado FabricPool .

Antes de começar

- Você deve ter a função de Administrador de Aplicativos 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 para ser gerado para essa exibição.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.

2. No menu Exibir, selecione **Desempenho > Todos os volumes**.
3. Selecione **Mostrar/Ocultar** para garantir que a coluna “Tipo de disco” apareça na exibição.

Adicione ou remova outras colunas para criar uma visualização importante para seu relatório.

4. Arraste a coluna “Tipo de disco” para perto da coluna “Dados frios”.
5. Clique no ícone de filtro, adicione o seguinte filtro e clique em **Aplicar filtro**:
 - Dados frios maiores que 100 GB
 - O 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) fique na parte inferior.
7. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo “Volumes de dados frios não FabricPool”.
8. Clique no botão **Relatórios agendados** na página de inventário.
9. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, você pode encontrar volumes que são bons candidatos para serem movidos para agregados do FabricPool .

Relatórios de exemplo do Microsoft Excel

Esses relatórios de exemplo do Microsoft Excel têm como objetivo apresentar opções de relatórios disponíveis usando recursos avançados do Excel.

A funcionalidade avançada do Excel pode criar uma ampla variedade de relatórios específicos para suas necessidades. Para obter informações completas sobre como usar o Excel, consulte a documentação do produto.



Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento para gerenciar relatórios.

Crie um relatório para mostrar uma tabela e um gráfico de capacidade agregada

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

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as seguintes etapas para abrir uma exibição Saúde: Todos os agregados, baixar a exibição no Excel, criar um gráfico de capacidade disponível, carregar o arquivo Excel personalizado e agendar o relatório final.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Agregados**.

2. Selecione **Relatórios > Baixar Excel**.



Dependendo do seu navegador, pode ser 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 planilha () depois do data planilha e nomeie-a como **Capacidade Total de Dados**.
6. Adicione as seguintes colunas na nova planilha 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 fórmula a seguir, certificando-se de que ela faça referência à planilha de dados (dados!) e aos especificadores de coluna e linha corretos para os dados capturados (a Capacidade Total de Dados extrai dados da coluna E, linhas 2 a 20).
 - a. =SOMA(dados!E\$2:dados!E\$20)
 - b. =SOMA(dados!F\$2:dados!F\$50)
 - c. =SOMA(dados!G\$2:dados!G\$50)
 - d. =SOMA(dados!H\$2:dados!H\$50)

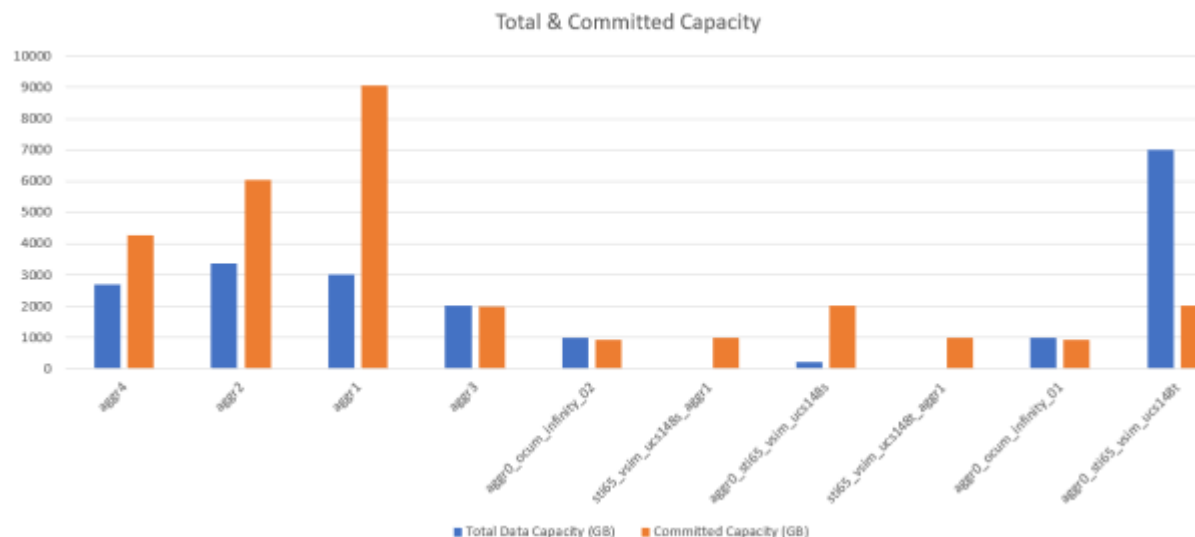
A fórmula totaliza cada coluna com base nos dados atuais.

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 planilha 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 **Colunas agrupadas**.
3. Clique com o botão direito do mouse no gráfico e selecione **Mover gráfico** para movê-lo para o Total Data Capacity folha.
4. Usando os menus **Design** e **Formato**, que estão disponíveis quando o gráfico é selecionado, você pode

personalizar a aparência do gráfico.

- Quando estiver satisfeito, salve o arquivo com suas alterações. Não altere o nome ou o local do arquivo.



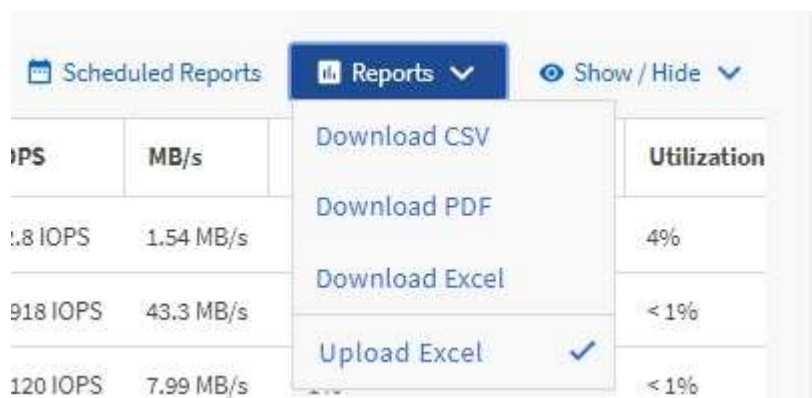
- No Unified Manager, selecione **Relatórios > Carregar Excel**.



Certifique-se de que você está na mesma visualização onde baixou o arquivo do Excel.

- Selecione o arquivo Excel que você modificou.
- Clique em **Abrir**.
- Clique em **Enviar**.

Uma marca de seleção aparece ao lado do item de menu **Relatórios > Carregar Excel**.



- Clique em **Relatórios agendados**.
- Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios para que você possa definir as características do agendamento para o novo relatório.



Selecione o formato **XLSX** para o relatório.

- Digite um nome para o agendamento 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 é gerado e enviado por e-

mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira investigar como usar melhor a capacidade disponível em sua rede.

Crie um relatório para mostrar gráficos de capacidade total agregada versus capacidade 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

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as seguintes etapas para abrir uma exibição Saúde: Todos os agregados, baixe a exibição no Excel, crie um gráfico de capacidade total e comprometida, carregue o arquivo Excel personalizado e agende o relatório final.

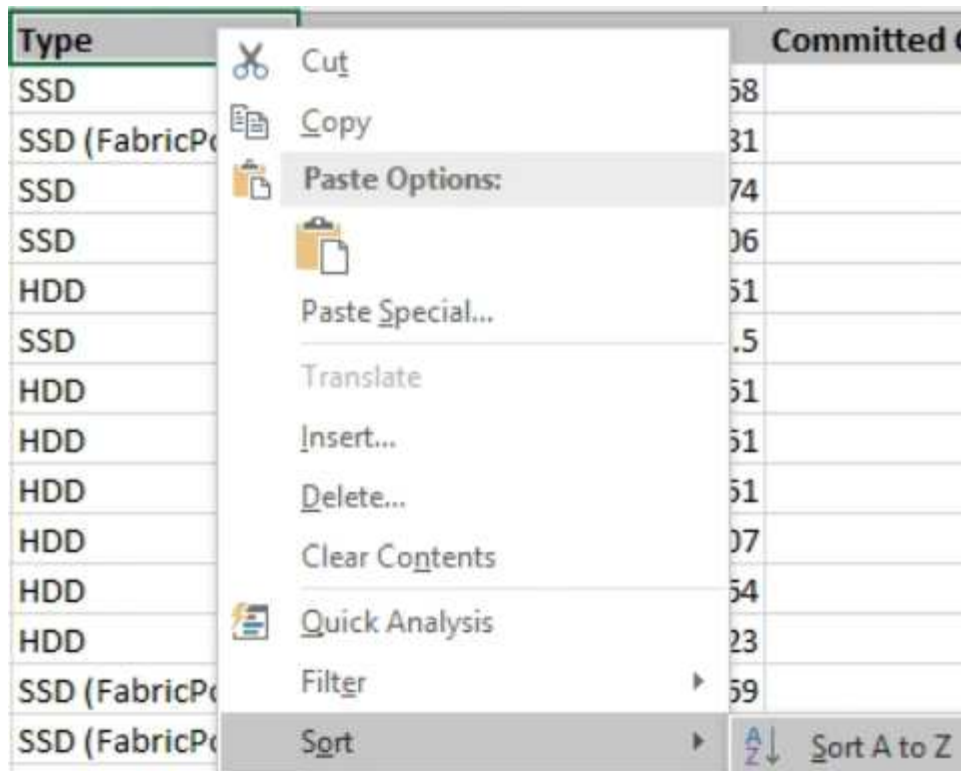
Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Agregados**.
2. Selecione **Relatórios > Baixar Excel**.



Dependendo do seu navegador, pode ser necessário clicar em **OK** para salvar o arquivo.

3. No Excel, abra o arquivo baixado.
4. Se necessário, clique em **Ativar edição**.
5. Na planilha de dados, clique com o botão direito do mouse na coluna Tipo e selecione **Classificar > Classificar de A a Z**.



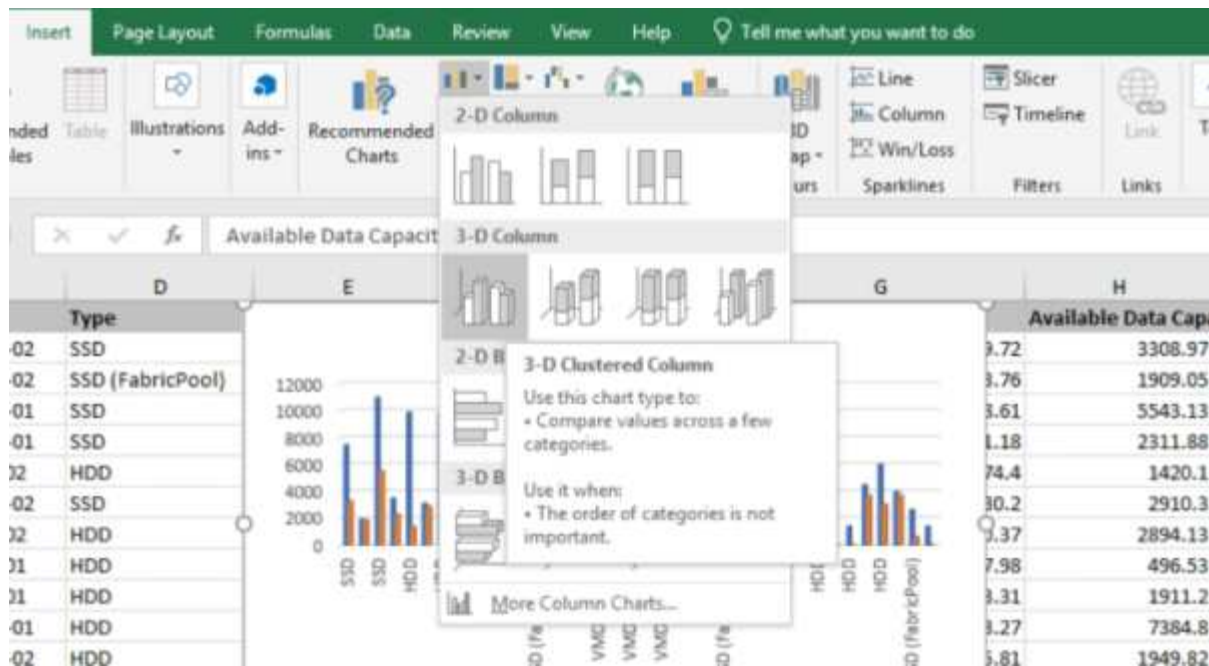
Isso organizará seus dados por tipo de armazenamento, como:

- HDD
- Híbrido
- SSD
- SSD (FabricPool)

6. Selecione o **Type**, **Total Data Capacity**, e **Available Data Capacity** colunas.

7. No menu **Inserir**, selecione um 3-D column gráfico.

O gráfico aparece na folha de dados.

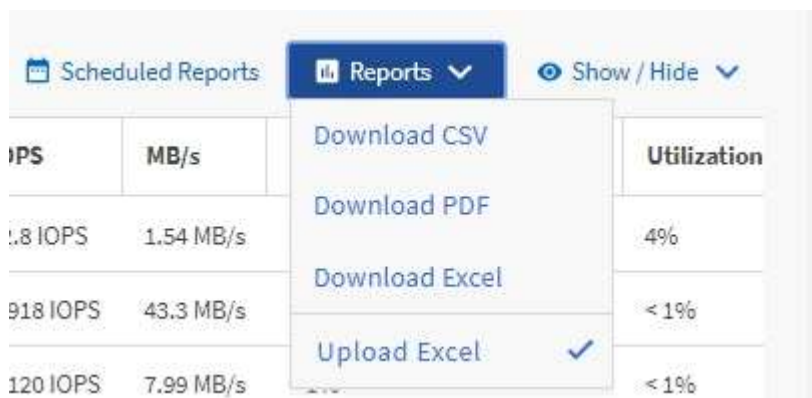




Certifique-se de que você está na mesma visualização onde baixou o arquivo do Excel.

14. Selecione o arquivo Excel que você modificou.
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 agendados**.
18. Clique em **Adicionar agendamento** para adicionar uma nova linha à página **Agendamentos de relatórios** para que você possa definir as características do agendamento para o novo relatório.



Selecione o formato **XLSX** para o relatório.

19. Digite um nome para o agendamento 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 é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira balancear a carga em seus agregados.

Crie um relatório para visualizar 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

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as seguintes etapas para abrir uma exibição Saúde: Todos os volumes, baixar a exibição no Excel, criar um gráfico de capacidade disponível, carregar o arquivo Excel personalizado e agendar o relatório final.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Volumes**.
2. Selecione **Relatórios > Baixar Excel**.



Dependendo do seu navegador, pode ser necessário clicar em **OK** para salvar o arquivo.

3. Se necessário, clique em **Ativar edição**.
4. No Excel, abra o arquivo baixado.
5. No data planilha, selecione os dados que deseja usar na Volume e Available Data % colunas.
6. No menu **Inserir**, selecione um 3-D piechart.

O gráfico mostra quais volumes têm o maior espaço disponível. O gráfico aparece na folha de dados.



Dependendo da configuração da sua rede, selecionar colunas inteiras ou muitas linhas de dados pode tornar seu gráfico de pizza ilegível. Este exemplo usa o gráfico de pizza 3D, mas você pode usar qualquer tipo de gráfico. Use o gráfico que melhor exibe os dados que você deseja capturar.

7. Nomeie o título do gráfico como **Capacidade disponível**.
8. Clique com o botão direito do mouse no gráfico e selecione **Mover gráfico**.
9. Selecione **Nova planilha** e nomeie a planilha como **Gráficos de volume de armazenamento**.



Certifique-se de que a nova planilha apareça depois das planilhas de informações e dados.



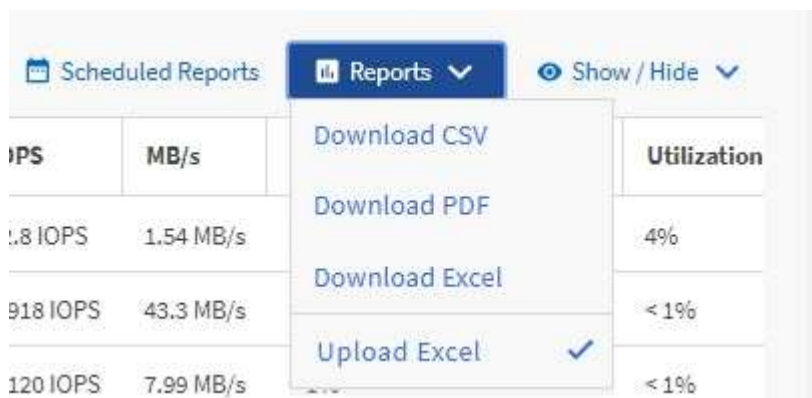
10. Usando os menus **Design** e **Formato**, disponíveis quando o gráfico é selecionado, você pode personalizar a aparência do gráfico.
11. Quando estiver satisfeito, salve o arquivo com suas alterações.
12. No Unified Manager, selecione **Relatórios > Carregar Excel**.



Certifique-se de que você está na mesma visualização onde baixou o arquivo do Excel.

13. Selecione o arquivo Excel que você 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 agendados**.
17. Clique em **Adicionar agendamento** para adicionar uma nova linha à página **Agendamentos de relatórios** para que você possa definir as características do agendamento para o novo relatório.
18. Digite um nome para o agendamento do relatório e preencha os outros campos do relatório e clique na marca de seleção (✓) no final da linha.



Selecione o formato **XLSX** para o relatório.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira balancear a carga em seus volumes.

Crie um relatório para visualizar agregados que tenham mais IOPS disponíveis

Este relatório mostra quais agregados têm mais IOPS disponíveis por tipo de agregado no qual você pode provisionar novas cargas de trabalho.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Use as seguintes etapas para abrir uma exibição Saúde: Todos os volumes, baixar a exibição no Excel, criar um gráfico de capacidade disponível, carregar o arquivo Excel personalizado e agendar o relatório final.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > Agregados**.
2. Selecione **Desempenho: Todos os agregados** no menu suspenso **Exibir**.
3. Selecione **Mostrar/Ocultar** para mostrar o Available IOPS coluna e ocultar o Cluster FQDN, Inactive Data Reporting, e Threshold Policy colunas.
4. Arraste e solte o Available IOPS e Free Capacity colunas ao lado do Type coluna.
5. Nomeie e salve a visualização personalizada Available IOPS Per Aggr.
6. Selecione **Relatórios > Baixar Excel**.



Dependendo do seu navegador, pode ser necessário clicar em **OK** para salvar o arquivo.

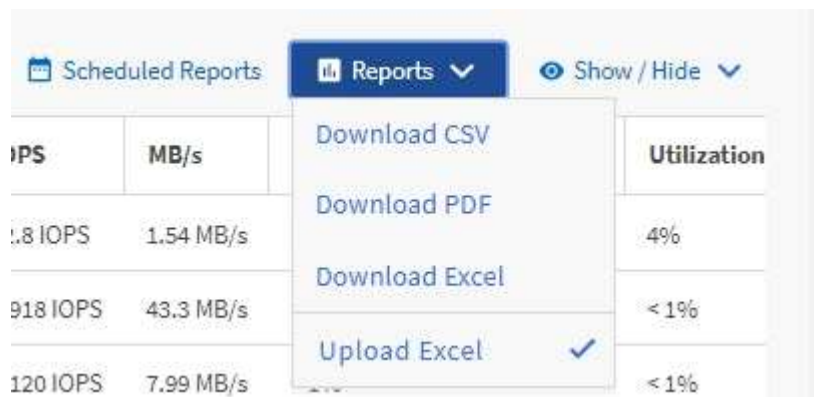
7. Se necessário, clique em **Ativar edição**.
8. No Excel, abra o arquivo baixado.
9. Na planilha de dados, clique no pequeno triângulo no canto superior esquerdo da planilha para selecionar a planilha inteira.
10. Na faixa de opções **Dados**, selecione **Classificar** na Sort & Filter area.
11. Defina os seguintes níveis de classificação:
 - a. Especifique **Classificar por** como Available IOPS (IOPS), o **Sort On** como Cell Values, e a **Ordem** como Largest to Smallest.
 - b. Clique em **Adicionar nível**.
 - c. Especifique **Classificar por** como Type, o **Classificar** como Cell Values, e a **Ordem** como Z to A.
 - d. Clique em **Adicionar nível**.
 - e. Especifique **Classificar por** como Free Capacity (GB), o **Classificar** como Cell Values, e a **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 visualização onde baixou o arquivo do Excel.

14. Selecione o arquivo Excel que você 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 agendados**.
18. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatórios para que você possa definir as características do agendamento para o novo relatório.
19. Digite um nome para o agendamento do relatório e preencha os outros campos do relatório e clique na marca de seleção (✓) no final da linha.



Selecione o formato **XLSX** para o relatório.

O relatório é enviado imediatamente como um teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados usando a frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira provisionar novas cargas de trabalho nos agregados que têm o maior IOPS disponível.

Gerenciar armazenamento usando APIs REST

Comece a usar as APIs Active IQ Unified Manager

O Active IQ Unified Manager fornece um conjunto de APIs para gerenciar seus recursos de armazenamento nos sistemas de armazenamento suportados por meio de uma interface de serviço web RESTful para qualquer integração de terceiros.

Nestes tópicos, você encontrará informações sobre APIs do Unified Manager, exemplos de fluxos de trabalho para resolver problemas específicos e alguns códigos de exemplo. Usando essas informações, você pode criar clientes RESTful de soluções de software NetApp Manageability para gerenciar sistemas NetApp. As APIs são baseadas no estilo arquitetônico Representational State Transfer (REST). Todas as quatro operações REST Criar, Ler, Atualizar e Excluir (também conhecidas como CRUD) são suportadas.

Ver ["Active IQ Unified Manager"](#) para obter recursos adicionais e detalhes sobre os benefícios da API REST do Active IQ Unified Manager.

Público para este conteúdo

Os tópicos aqui são destinados a desenvolvedores que criam aplicativos que interagem com o software Active IQ Unified Manager por meio de APIs REST.

Administradores e arquitetos de armazenamento podem consultar essas informações para obter uma compreensão básica de como as APIs REST do Unified Manager podem ser usadas para criar aplicativos cliente para gerenciar e monitorar sistemas de armazenamento NetApp.

Você deve usar essas informações se quiser usar o provedor de armazenamento, o cluster ONTAP e as APIs de administração de gerenciamento para gerenciar seu armazenamento.



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 e categorias da API do Active IQ Unified Manager

As APIs do Active IQ Unified Manager permitem que você gerencie e provisione objetos de armazenamento em seu ambiente. Você também pode acessar a interface da Web do Unified Manager para executar algumas dessas funções.

Construir uma URL para acessar diretamente as APIs REST

Você pode acessar as APIs REST diretamente por meio de uma linguagem de programação, como Python, C#, C++, JavaScript e assim por diante. Insira o nome do host ou endereço IP e a URL para acessar as APIs REST no formato

`https://<nome do host>/api`



A porta padrão é 443. Você pode configurar a porta conforme exigido pelo seu ambiente.

Acesse a página de documentação da API online

Você pode acessar a página de conteúdo de referência *Documentação da API* que acompanha 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 endereço IP e a URL para acessar a página da API REST no formato

`https://<nome do host>/docs/api/`

Categorias

As chamadas de API são organizadas funcionalmente com base em áreas ou categorias. Para localizar uma API específica, clique na categoria de API aplicável.

As APIs REST fornecidas com o Unified Manager ajudam você a executar funções administrativas, de monitoramento e provisionamento. As APIs são agrupadas nas seguintes categorias.

- **centro de dados**

Esta categoria contém as APIs que ajudam você no gerenciamento e análise de armazenamento do datacenter usando 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 seu data center.

- **servidor de gerenciamento**

As APIs na categoria **management-server** contêm o `jobs`, `system`, e `events` APIs. Trabalhos são operações agendadas para execução assíncrona relacionadas ao gerenciamento de objetos de armazenamento ou cargas de trabalho no Unified Manager. O `events` A API retorna eventos no seu data center e o `system` A API retorna os detalhes da instância do Unified Manager.

- **provedor de armazenamento**

Esta categoria contém todas as APIs de provisionamento necessárias para gerenciar e provisionar compartilhamentos de arquivos, LUNs, níveis de serviço de desempenho e políticas de eficiência de armazenamento. 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 armazenamento.

- **administração**

Esta categoria contém as APIs usadas para executar tarefas administrativas, como manter configurações de backup, visualizar certificados de armazenamento confiável para as fontes de dados do Unified Manager e gerenciar clusters ONTAP como fontes de dados para o Unified Manager.

- **portal**

O Unified Manager permite que você invoque APIs REST do ONTAP por meio das APIs na categoria gateway e gerencie os objetos de armazenamento no seu data center.

- **segurança**

Esta categoria contém APIs para gerenciar usuários do Unified Manager.

Serviços REST oferecidos no 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 operações de leitura (GET) ou gravação (POST, PATCH, DELETE). A seguir estão alguns exemplos das operações GET, PATCH, POST e DELETE suportadas pelas APIs:

- Exemplo para GET: `GET /datacenter/cluster/clusters` recupera detalhes do cluster no seu data center. O número máximo de registros retornados pelo GET a operação é 1000.



As APIs permitem que você filtre, classifique e ordene os registros por atributos suportados.

- Exemplo para POST: `POST /datacenter/svm/svms` cria uma Máquina Virtual de Armazenamento (SVM) personalizada.
- Exemplo para PATCH: `PATCH /datacenter/svm/svms/{key}` modifica as propriedades de uma SVM, usando sua chave exclusiva.
- Exemplo para DELETE: `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 Aplicativo.

Função do usuário	Método REST suportado
Operador	Acesso somente leitura aos dados. Usuários com essa função podem executar todas as solicitações GET.
Administrador de Armazenamento	Acesso de leitura a todos os dados. Usuários com essa função podem executar todas as solicitações GET. Além disso, eles têm acesso de gravação (para executar solicitações PATCH, POST e DELETE) para executar atividades específicas, como gerenciamento de objetos de serviço de armazenamento e opções de gerenciamento de armazenamento.
Administrador do aplicativo	Acesso de leitura e gravação a todos os dados. 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

Os URIs da API REST no Active IQ Unified Manager especificam 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 impacto 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 aos lançamentos. URIs com um número de versão fornecem uma interface consistente que mantém a compatibilidade com 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 básicas 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 que você use a versão mais recente de uma API específica (em relação ao número inteiro incremental) disponível na sua 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 manipular. Em solicitações REST, você deve incluir o parâmetro de versão. As versões anteriores das APIs acabam sendo descontinuadas após alguns lançamentos. Nesta versão, o `v1` versão das APIs está obsoleta.

Recursos de armazenamento no ONTAP

Os recursos de armazenamento no ONTAP podem ser amplamente classificados em *recursos de armazenamento físico* e *recursos de armazenamento lógico*. Para gerenciar efetivamente seus sistemas ONTAP usando as APIs fornecidas no Active IQ Unified Manager, você deve entender o modelo de recurso de armazenamento e o relacionamento entre vários recursos de armazenamento.

- **Recursos de armazenamento físico**

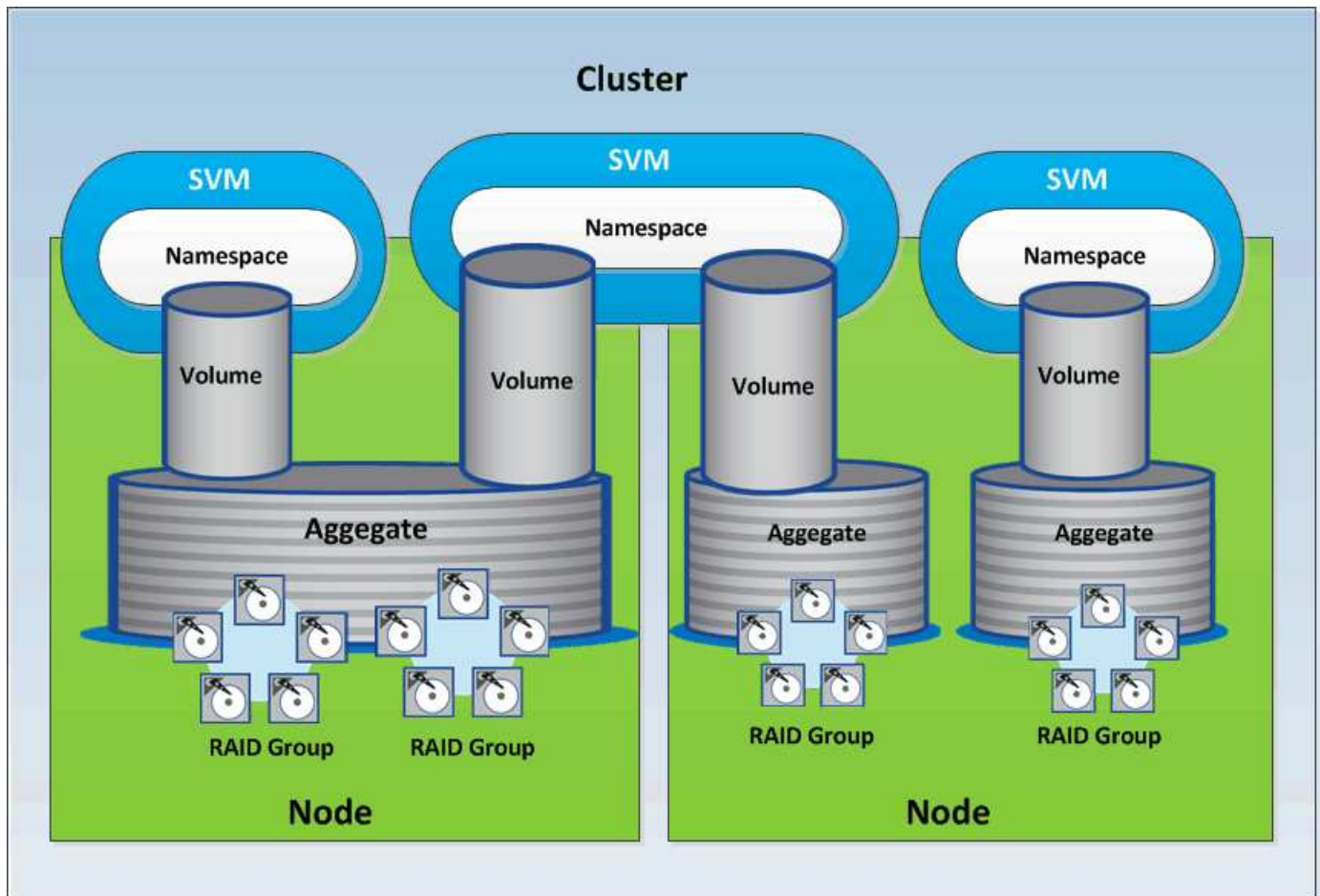
Refere-se aos objetos de armazenamento físico fornecidos pelo ONTAP. Os recursos de armazenamento físico incluem discos, clusters, controladores de armazenamento, nós e agregados.

- **Recursos de armazenamento lógico**

Refere-se aos recursos de armazenamento fornecidos pelo ONTAP que não estão vinculados a um recurso físico. Esses recursos estão associados a uma máquina virtual de armazenamento (SVM, anteriormente conhecida como Vserver) e existem independentemente de qualquer recurso de armazenamento físico específico, como um disco, LUN de matriz ou agregado.

Os recursos de armazenamento lógico incluem volumes de todos os tipos e qtrees, bem como os recursos e configurações que você pode usar com esses recursos, como cópias de instantâneo, deduplicação, compactação e cotas.

A ilustração a seguir mostra os recursos de armazenamento em um cluster de 2 nós:



Acesso e autenticação da API REST no Active IQ Unified Manager

A API REST do Active IQ Unified Manager pode ser acessada usando qualquer cliente REST ou plataforma de programação que possa emitir solicitações HTTP com um mecanismo básico de autenticação HTTP.

Um exemplo de solicitação e resposta:

- **Solicitar**

```
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 de 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 plug-ins de navegador da API REST. Você também pode acessar a API REST usando plataformas de script como cURL e Perl.

Autenticação

O Unified Manager oferece suporte ao esquema básico de autenticação HTTP para APIs. Para um fluxo seguro de informações (solicitação e resposta), as APIs REST são acessíveis somente via 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 invocar 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 via LDAP). Você pode gerenciar o acesso do usuário efetuando

login na interface do usuário do Console de administração do Unified Manager.

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 configuração do Active Directory.
202	Aceito	Retornado na execução bem-sucedida de chamadas assíncronas para funções de provisionamento, como criação de LUNs e compartilhamentos de arquivos.
400	Solicitação inválida	Indica falha na validação de entrada. O usuário precisa corrigir as entradas, por exemplo, chaves válidas no corpo de uma 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 estava tentando acessar não foi encontrado.
405	Método não permitido	Método não permitido.
429	Muitas solicitações	Retornado quando o usuário envia muitas solicitações em um período específico.

Código de status HTTP	Título do código de status	Descrição
500	Erro do Servidor Interno	Erro do Servidor Interno. Falha ao obter resposta do servidor. Este erro interno do servidor pode ou não ser permanente. Por exemplo, se você executar um GET ou GET ALL operação e receber esse erro, é recomendável repetir essa operação por no mínimo cinco tentativas. Se for um erro permanente, o código de status retornado continua sendo 500. Se a operação for bem-sucedida, o código de status retornado será 200.

Recomendações para usar as APIs do Active IQ Unified Manager

Ao usar as APIs no Active IQ Unified Manager, você deve seguir determinadas práticas recomendadas.

- Todo 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 ao 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 matriz usando uma API do Unified Manager, você deve atualizar toda a sequência de valores. Não é possível anexar valores a uma matriz. Você só pode substituir uma matriz existente.
- Você pode usar operadores de filtro, como pipe (|) e curinga (*) 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 curinga (*) e barra vertical (|). Ele pode recuperar um número incorreto de objetos.
- Ao usar valores para filtro, certifique-se de que o valor não contenha nenhum ? personagem. Isso é para mitigar riscos de injeção de SQL.
- Note que o GET (todas) as solicitações de qualquer API retornam no máximo 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 interface do usuário do Unified Manager.

Registros para solução de problemas

Os logs do sistema permitem que você analise as causas de falhas e solucione 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 log	Usar
<code>/var/log/ocie/access_log.log</code>	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. Você pode usar este arquivo de log para verificar as APIs usadas com frequência ou solucionar problemas de qualquer fluxo de trabalho da GUI. Você também pode usá-lo para dimensionar a análise, com base no tempo de execução.
<code>/var/log/ocum/ocumserver.log</code>	Contém todos os logs de execução da API. Você pode usar este arquivo de log para solucionar problemas e depurar chamadas de API.
<code>/var/log/ocie/server.log</code>	Contém todas as implantações do servidor Wildfly e logs relacionados ao serviço de início/parada. Você pode usar este arquivo de log para encontrar a causa raiz de quaisquer problemas que ocorram durante a inicialização, parada ou implantação do servidor Wildfly.
<code>/var/log/ocie/au.log</code>	Contém registros relacionados à unidade de aquisição. Você pode usar este arquivo de log quando tiver criado, modificado ou excluído quaisquer objetos no ONTAP , mas eles não serão refletidos nas APIs REST do Active IQ Unified Manager .

Objetos de trabalho processos assíncronos

O Active IQ Unified Manager fornece o `jobs` API que recupera informações sobre os trabalhos realizados durante a execução de outras APIs. Você deve saber como o processamento assíncrono funciona usando o objeto Job.

Algumas chamadas de API, especialmente 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 de forma assíncrona.

Solicitações assíncronas descritas usando o objeto Job

Após realizar uma chamada de API 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 em execução após a resposta HTTP inicial ao cliente. A resposta inclui o objeto Job que ancora a solicitação, incluindo seu identificador exclusivo.

Consultar o objeto Job associado a uma solicitação de API

O objeto Job retornado na resposta HTTP contém diversas propriedades. Você pode consultar a propriedade `state` para determinar se a solicitação foi concluída com sucesso. Um objeto Job pode estar em um dos seguintes estados:

- `NORMAL`
- `WARNING`
- `PARTIAL_FAILURES`
- `ERROR`

Há duas técnicas que você pode usar ao pesquisar um objeto Job para detectar um estado terminal para a tarefa, seja sucesso ou falha:

- Solicitação de pesquisa padrão: o estado atual do trabalho é retornado imediatamente.
- Solicitação de pesquisa longa: quando o estado do trabalho muda para `NORMAL`, `ERROR`, ou `PARTIAL_FAILURES`.

Etapas em uma solicitação assíncrona

Você pode usar o seguinte procedimento de alto nível para concluir uma chamada de API assíncrona:

1. Emita a chamada de API assíncrona.
2. Receba uma resposta HTTP 202 indicando aceitação bem-sucedida da solicitação.
3. Extraia o identificador do objeto Job do corpo da resposta.
4. Dentro de um loop, aguarde o objeto Job atingir o estado terminal `NORMAL`, `ERROR`, ou `PARTIAL_FAILURES`.
5. Verifique o estado 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` formatar).

O URI usado é: <https://<hostname>/api/datacenter/svm/svms>. Este código de exemplo usa os seguintes parâmetros de entrada:

- O endereço IP ou FQDN do servidor API
- Opcional: Número da porta (padrão: 443)
- Nome de usuário
- Senha
- Formato de resposta(`application/json`)

Para invocar APIs REST, você também pode usar outros scripts, como Jersey e RESTEasy, para escrever um cliente Java REST para o 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
- Usos `javax.net.ssl.HttpsURLConnection` para uma conexão URI
- Usa uma biblioteca de terceiros(`org.apache.commons.codec.binary.Base64`) para construir a string codificada em 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.HttpsURLConnection;
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 {
        HttpsURLConnection 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 =
(HttpURLConnection) 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 o Active IQ Unified Manager estão listadas nesta seção, com base em suas categorias.

Você pode visualizar a página de documentação on-line da sua instância do Unified Manager que inclui os detalhes de cada chamada da 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 em 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 até o final da página e clique na categoria de API aplicável.

- Verbo HTTP (chamar)

O verbo HTTP identifica a ação realizada em um recurso. Cada chamada de API é executada por meio de

um único verbo HTTP.

- Caminho

O caminho determina o recurso específico que a ação usa como parte da execução de uma chamada. A string do caminho é anexada à URL principal para formar a URL completa que identifica o recurso.

Gerenciar objetos de armazenamento em um data center usando APIs

As APIs REST sob o `datacenter` A categoria permite que você gerencie os objetos de armazenamento no seu data center, como clusters, nós, agregados, VMs de armazenamento, 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 adicionar, excluir ou modificar esses objetos.

A maioria dessas APIs são chamadas GET que fornecem agregação entre clusters com suporte para filtragem, classificação e paginação. Ao executar essas APIs, elas retornam dados do banco de dados. Portanto, os objetos recém-criados precisam ser descobertos pelo próximo ciclo de aquisição para aparecerem na resposta.

Se 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 de métricas e análises dos objetos de armazenamento, consulte ["Visualizando métricas de desempenho"](#).

```
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 sua interface de API do Swagger. Você pode filtrar e ordenar os resultados por parâmetros específicos, conforme indicado no Swagger. Essas APIs permitem filtrar os resultados para objetos de armazenamento específicos, como cluster, volume ou VM de armazenamento.

APIs para objetos de armazenamento em seu data center

verbo HTTP	Caminho	Descrição
GET	<code>/datacenter/cluster/clusters</code> <code>/datacenter/cluster/clusters/{key}</code>	Você pode usar este método para visualizar os detalhes dos clusters 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	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	Retorna os detalhes das licenças instaladas nos clusters do seu data center. Você pode filtrar seus resultados com base nos critérios necessários. Informações como chave de licença, chave de cluster, data de expiração e escopo da licença são retornadas. Você pode inserir uma chave de licença para recuperar os detalhes de uma licença específica.
GET	/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}	Você pode usar este método para visualizar os detalhes dos nós no data center. Você pode visualizar informações sobre o cluster, a integridade do nó, a capacidade de desempenho e o par de alta disponibilidade (HA) do nó.
GET	/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}	Você pode usar este método para visualizar os detalhes dos compartilhamentos CIFS no data center. Além dos detalhes do cluster, SVM e volume, informações sobre a Lista de Controle de Acesso (ACL) também são retornadas.
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	Você pode usar este método para visualizar os detalhes das políticas de exportação para os serviços NFS suportados. Você pode consultar as políticas de exportação de um cluster ou VM de armazenamento e reutilizar a chave da política de exportação para provisionar compartilhamentos de arquivos NFS. Para obter mais informações sobre como atribuir e reutilizar políticas de exportação em cargas de trabalho, consulte “Provisionando compartilhamentos de arquivos CIFS e NFS”.

verbo HTTP	Caminho	Descrição
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	Você pode usar esse método para visualizar a coleção de agregados no data center ou um agregado específico para provisionar cargas de trabalho neles ou monitorar. Informações como detalhes do cluster e do nó, capacidade de desempenho usada, espaço disponível e usado e eficiência de armazenamento são retornadas.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	Você pode usar este método para visualizar a coleção de LUNs em todo o data center. Você pode visualizar informações sobre o LUN, como detalhes do cluster e do SVM, políticas de QoS e igroups.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	Você pode usar este método para visualizar os detalhes de todas as políticas de QoS aplicáveis aos objetos de armazenamento no data center. Informações como detalhes do cluster e do SVM, detalhes da política fixa ou adaptável e número de objetos aplicáveis a essa política são retornadas.
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	Você pode usar este método para visualizar os detalhes do qtree no data center para todos os volumes FlexVol ou FlexGroup . Informações como detalhes do cluster e do SVM, FlexVol volume e política de exportação são retornadas.

verbo HTTP	Caminho	Descrição
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	Você pode usar este método para visualizar a coleção de volumes no data center. Informações sobre os volumes, como detalhes do SVM e do cluster, QoS e políticas de exportação, e se o volume é do tipo leitura-gravação, proteção de dados ou compartilhamento de carga, são retornadas. Para volumes FlexVol e FlexClone , você pode visualizar as informações sobre os respectivos agregados. Para um volume FlexGroup , a consulta retorna a lista de agregados constituintes.
GET POST DELETE PATCH	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}	Você pode atribuir grupos iniciadores (igroups) autorizados a acessar destinos LUN específicos. Se houver um igroup existente, você poderá atribuí-lo. Você também pode criar igroups e atribuí-los aos LUNs. Você pode usar esses métodos para consultar, criar, excluir e modificar igroups, respectivamente. Pontos a serem observados: • POST: Ao criar um igroup, você pode designar a VM de armazenamento à qual deseja atribuir acesso. • DELETE: Você precisa fornecer a chave igroup como um parâmetro de entrada para excluir um igroup específico. Se você já atribuiu um igroup a um LUN, não poderá excluir esse igroup. • PATCH: Você precisa fornecer a chave igroup como um parâmetro de entrada para modificar um igroup específico. Você também deve inserir o imóvel que deseja atualizar, juntamente com seu valor.

verbo HTTP	Caminho	Descrição
GET	/datacenter/svm/svms	Você pode usar esses métodos para visualizar, criar, excluir e modificar Máquinas Virtuais de Armazenamento (VMs de armazenamento). • POST: Você deve inserir o objeto de VM de armazenamento que deseja criar como um parâmetro de entrada. Você pode criar uma VM de armazenamento personalizada e, em seguida, atribuir as propriedades necessárias a ela. • DELETE: Você precisa fornecer a chave da VM de armazenamento para excluir uma VM de armazenamento específica. • PATCH: Você precisa fornecer a chave da VM de armazenamento para modificar uma VM de armazenamento específica. Você também precisa inserir as propriedades que deseja atualizar, juntamente com seus valores.
POST	/datacenter/svm/svms/{key}	
DELETE		
PATCH		



Pontos a serem observados:

Se você tiver habilitado o provisionamento de carga de trabalho baseado em SLO em seu ambiente, ao criar a VM de armazenamento, certifique-se de que ela ofereça suporte a todos os protocolos necessários para provisionar LUNs e compartilhamentos de arquivos nelas, por exemplo, CIFS ou SMB, NFS, FCP e iSCSI. Os fluxos de trabalho de provisionamento podem falhar se a VM de armazenamento não oferecer suporte aos serviços necessários. É recomendável que os serviços para os respectivos tipos de cargas de trabalho também sejam habilitados na VM de armazenamento.

Se você tiver habilitado o provisionamento de carga de trabalho baseado em SLO em seu ambiente, não poderá excluir a VM de armazenamento na qual as cargas de trabalho de armazenamento foram provisionadas. Quando você exclui uma VM de armazenamento na qual um servidor CIFS ou SMB foi configurado, esta API também exclui o servidor CIFS ou SMB, juntamente com a configuração local do Active Directory. No entanto, o nome do servidor CIFS ou SMB continua na configuração do Active Directory que você deve excluir manualmente do servidor do Active Directory.

APIs para elementos de rede em seu data center

As seguintes APIs na categoria datacenter 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	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	Recupera informações sobre todas as portas Ethernet no seu ambiente de data center. Com uma chave de porta como parâmetro de entrada, você pode visualizar as informações dessa porta específica. Informações, como detalhes do cluster, domínio de transmissão, detalhes da porta, como estado, velocidade e tipo, e se a porta está habilitada, são recuperadas.
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	Você pode usar este método para visualizar os detalhes das interfaces FC no seu ambiente de data center. Com uma chave de interface como parâmetro de entrada, você pode visualizar as informações dessa interface específica. Informações, como detalhes do cluster, detalhes do nó inicial e detalhes da porta inicial, são recuperadas.
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	Recupera informações sobre todas as portas FC usadas nos nós do seu ambiente de data center. Com uma chave de porta como parâmetro de entrada, você pode visualizar as informações dessa porta específica. Informações como detalhes do cluster, descrição da porta, protocolo suportado e estado da porta são recuperadas.
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	Você pode usar este método para visualizar os detalhes das interfaces IP no seu ambiente de data center. Com uma chave de interface como parâmetro de entrada, você pode visualizar as informações dessa interface específica. Informações como detalhes do cluster, detalhes do IPspace, detalhes do nó inicial e se o failover está habilitado são recuperadas.

Acesse APIs ONTAP por meio de acesso proxy

As APIs de gateway oferecem a vantagem de usar as credenciais do Active IQ Unified Manager para executar APIs REST do ONTAP e gerenciar objetos de armazenamento. Essas APIs estão disponíveis quando o recurso API Gateway é habilitado na interface da Web do Unified Manager.

As APIs REST do Unified Manager oferecem suporte apenas a um conjunto selecionado de ações a serem executadas nas fontes de dados do Unified Manager, ou seja, clusters ONTAP . Você pode aproveitar os outros recursos por meio das APIs ONTAP . As APIs de gateway permitem que o Unified Manager seja uma interface de passagem para encapsular todas as solicitações de API a serem executadas em clusters ONTAP que ele gerencia, sem precisar efetuar login em cada cluster de data center individualmente. Ele funciona como um único ponto de gerenciamento para executar as APIs nos clusters 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 precisar fazer login neles individualmente. As APIs de gateway permitem que você permaneça conectado ao Unified Manager e gerencie os clusters ONTAP executando operações da 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 encapsular as solicitações de API, mantendo o cabeçalho e o corpo das solicitações no mesmo formato das APIs ONTAP . Você pode usar suas credenciais do Unified Manager e executar operações específicas para acessar e gerenciar os clusters ONTAP sem passar credenciais de cluster individuais. Ele continua gerenciando a autenticação e o gerenciamento do 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	Este método GET recupera a lista de todos os clusters gerenciados pelo Unified Manager que suportam chamadas ONTAP REST. Você pode verificar os detalhes do cluster e optar por executar outros métodos com base no UUID do cluster ou no identificador exclusivo universal (UUID).  As APIs de gateway recuperam apenas os clusters suportados pelo ONTAP 9.5 ou posterior e adicionados ao Unified Manager por HTTPS.

verbo HTTP	Caminho (URL)	Descrição
GET POST DELETE PATCH OPTIONS(não disponível no Swagger) HEAD(não disponível no Swagger)	/gateways/{uuid}/{path}  O valor de {uuid} deve ser substituído pelo UUID do cluster no qual a operação REST deve ser executada. Além disso, certifique-se de que o UUID seja do cluster suportado pelo ONTAP 9.5 ou posterior e adicionado ao Unified Manager por HTTPS. {path} deve ser substituído pelo URL REST do ONTAP. Você deve remover /api/ da URL.	Esta é uma API proxy de ponto único, que suporta operações POST, DELETE, PATCH e GET para todas as APIs REST do ONTAP. Nenhuma restrição se aplica a nenhuma API, desde que seja suportada pelo ONTAP. A funcionalidade de tunelamento ou proxy não pode ser desabilitada. O OPTIONS O método retorna todas as operações suportadas por uma API REST ONTAP. Por exemplo, se uma API ONTAP suporta apenas o GET operação, executando o OPTIONS método usando esta API de gateway retorna GET como resposta. Este método não é suportado no Swagger, mas pode ser executado em outras ferramentas de API. O OPTIONS O 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.

Entenda o tunelamento do API Gateway

As APIs de gateway permitem que você gerencie objetos ONTAP por meio do Unified Manager. O Unified Manager gerencia os clusters e os detalhes de autenticação e redireciona as solicitações para o ponto de extremidade REST do ONTAP. A API do gateway transforma a URL e o Hypermedia como o mecanismo do estado do aplicativo (HATEOAS) vincula o cabeçalho e o corpo da resposta com a URL base do gateway da API. A API do gateway atua como a URL base do proxy à qual você anexa a URL REST do ONTAP e executa o ponto de extremidade REST do ONTAP necessário.



Para que uma API ONTAP seja executada com sucesso por meio do gateway de API, a API deve ser suportada pela versão do cluster ONTAP no qual está sendo executada. Executar uma API que não é suportada no cluster ONTAP não retorna nenhum resultado.

Neste exemplo, a API do gateway (URL base do proxy) é: /gateways/{uuid}/

A API ONTAP adotada é: /storage/volumes. Você precisa adicionar a URL REST da API ONTAP como valor para o parâmetro de caminho.



Ao adicionar o caminho, certifique-se de ter removido o “/” symbol at the beginning of the URL. For the API `/storage/volumes`, adicionar `storage/volumes`.

O URL anexado é: `/gateways/{uuid}/storage/volumes`

Ao executar o GET operação, a URL gerada é a seguinte:

`GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes`

O `/api` a tag da URL REST do ONTAP é removida na URL anexada e a da API do gateway é mantida.

Exemplo de comando cURL

```
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 ONTAP REST.

Definir escopo da API

Todas as APIs têm um contexto definido dentro do escopo do cluster. As APIs que operam com base em VMs de armazenamento também têm o cluster como escopo, ou seja, as operações da API são executadas em uma VM de armazenamento específica dentro de um cluster gerenciado. Quando você executa o `/gateways/{uuid}/{path}` API, certifique-se de inserir o UUID do cluster (UUID da fonte de dados do Unified Manager) 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 da 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 filtro no cabeçalho da string e a operação é executada dentro do escopo dessa VM de armazenamento dentro desse cluster.

Exemplo de comando cURL

```
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 o uso de APIs REST do ONTAP, consulte <https://docs.netapp.com/us-en/ontap-automation/index.html>["Automação de API REST ONTAP"]

Executar tarefas administrativas usando APIs

Você pode usar as APIs sob o `administration` categoria para modificar configurações de backup, verificar as informações do arquivo de backup e certificados de cluster, e também gerenciar clusters ONTAP como fontes de dados do Active IQ Unified Manager.



Você deve ter a função de Administrador do Aplicativo para executar essas operações. Você também pode usar a interface da Web do Unified Manager para definir essas configurações.

verbo HTTP	Caminho	Descrição
GET PATCH	/admin/backup-settings /admin/backup-settings	Você pode usar o GET método para visualizar as configurações do agendamento de backup definido no Unified Manager por padrão. Você pode verificar o seguinte: • Se a programação está habilitada ou desabilitada • Frequência do backup agendado (diária ou semanal) • Hora do backup • Número máximo de arquivos de backup que devem ser mantidos no aplicativo O horário do backup está no fuso horário do servidor. 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.
GET	/admin/backup-file-info	Um arquivo de despejo de backup é gerado sempre que o agendamento de backup é modificado para o Unified Manager. Você pode usar este método para verificar se o arquivo de backup foi gerado de acordo com as configurações de backup modificadas e se as informações no arquivo correspondem às configurações modificadas.

verbo HTTP	Caminho	Descrição
GET	/admin/datasource-certificate	Você pode usar este método para visualizar o certificado da fonte de dados (cluster) do armazenamento confiável. A validação do certificado é necessária antes de adicionar um cluster ONTAP como uma fonte de dados do Unified Manager.
GET POST PATCH DELETE	/admin/datasources/clusters /admin/datasources/clusters/{key}	Você pode usar o GET método para recuperar os detalhes das fontes de dados (clusters 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 precisa 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 ONTAP .

Gerenciar usuários usando APIs

Você pode usar as APIs no `security` 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 ou grupos remotos que pertencem a um servidor de autenticação. Com base nos privilégios das funções que você atribui aos usuários, eles podem gerenciar os objetos de armazenamento ou visualizar os dados no Unified Manager.



Você deve ter a função de Administrador do Aplicativo para executar essas operações. Você também pode usar a interface da Web do Unified Manager para definir essas configurações.

As APIs sob o `security` categoria usa o parâmetro `users`, que é o nome do usuário, e não o parâmetro `key` como identificador exclusivo para a entidade do usuário.

verbo HTTP	Caminho	Descrição
GET POST	 /security/users	Você pode usar esses métodos para obter detalhes dos usuários ou adicionar novos usuários 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, o usuário de manutenção e o usuário do banco de dados.
GET PATCH DELETE	/security/users/{name}	O método GET permite que você recupere todos os detalhes de um usuário, como nome, endereço de e-mail, função e tipo de autorização. O método PATCH permite que você atualize os detalhes. O método DELETE permite que você remova o usuário.

Visualizar métricas de desempenho usando APIs

O Active IQ Unified Manager fornece um conjunto de APIs sob o `/datacenter` categoria que permite visualizar os dados de desempenho dos seus clusters e objetos de armazenamento em um data center. Essas APIs recuperam os dados de desempenho de diferentes objetos de armazenamento, como clusters, nós, LUNs, volumes, agregados, VMs de armazenamento, interfaces FC, portas FC, portas Ethernet e interfaces IP.

O `/metrics` e `/analytics` As APIs fornecem diferentes visões das métricas de desempenho, usando as quais você pode detalhar diferentes níveis dos seguintes objetos de armazenamento no seu data center:

- aglomerados
- nós
- VMs de armazenamento
- agregados
- volumes
- LUNs
- Interfaces FC
- Portas FC
- Portas Ethernet
- Interfaces IP

A tabela a seguir faz uma comparação entre os `/metrics` e `/analytics` APIs com relação aos detalhes dos dados de desempenho recuperados.

Métricas	Análise
Detalhes de desempenho para um único objeto. Por exemplo, o <code>/datacenter/cluster/clusters/{key}/metrics</code> API exige que a chave do 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, o <code>/datacenter/cluster/clusters/analytics</code> API recupera as métricas coletivas de todos os clusters em um data center.
Exemplo 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 desempenho para um determinado tipo de objeto de armazenamento por um determinado período (acima de 72 horas).
Detalhes básicos do objeto são recuperados, como detalhes de um nó ou cluster.	Nenhum detalhe específico é recuperado.
Contadores acumulados, como mínimo, máximo, 95º percentil e valores médios de desempenho ao longo de um período de tempo, são recuperados para um único objeto, como contadores de leitura, gravação, total e outros.	Um único valor agregado é exibido para todos os objetos do mesmo tipo.

Métricas	Análise
O intervalo de tempo e os dados de amostra são baseados no seguinte cronograma: O intervalo de tempo para os dados. Exemplos podem ser 1h, 12h, 1d, 2d, 3d, 15d, 1s, 1m, 2m, 3m, 6m. Você obtém amostras de 1 hora se o intervalo for maior que 3 dias (72 horas); caso contrário, são amostras de 5 minutos. O período para cada intervalo de tempo é o seguinte: • 1h: Métricas da hora mais recente amostradas em 5 minutos. • 12h: Métricas das últimas 12 horas amostradas em 5 minutos. • 1d: Métricas do dia mais recente amostradas ao longo de 5 minutos. • 2d: Métricas dos últimos 2 dias amostradas ao longo de 5 minutos. • 3d: Métricas dos últimos 3 dias amostradas em 5 minutos. • 15d: Métricas dos últimos 15 dias amostradas em 1 hora. • 1 semana: métricas da semana mais recente amostradas ao longo de 1 hora. • 1m: Métricas do mês mais recente amostradas ao longo de 1 hora. • 2m: Métricas dos últimos 2 meses amostradas ao longo de 1 hora. • 3m: Métricas dos últimos 3 meses amostradas ao longo de 1 hora. • 6m: Métricas dos últimos 6 meses amostradas ao longo de 1 hora. Valores disponíveis: 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m Valor padrão: 1h	Acima de 72 horas. A duração durante a qual esta amostra é calculada é representada no formato padrão ISO-8601.

Exemplo de saída para APIs de métricas

Por exemplo, o `/datacenter/cluster/nodes/{key}/metrics` API recupera os seguintes detalhes (entre outros) para um nó:



O percentil 95 no valor resumido indica que 95% das amostras coletadas no 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
}
},
```

Exemplo de saída para APIs de análise

Por exemplo, o `/datacenter/cluster/nodes/analytics` AAPI 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 de APIs disponíveis

A tabela a seguir descreve o `/metrics` e `/analytics` APIs em detalhes.



As métricas de IOPS e desempenho retornadas por essas APIs são valores duplos, por exemplo 100.53. Não há suporte para filtrar esses valores flutuantes pelos caracteres pipe (|) e curinga (*).

Verbo HTTP	Caminho	Descrição
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 o UUID, intervalo de tempo, IOPS, taxa de transferência e 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 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 o UUID do nó, intervalo de tempo, resumo do IOPS, taxa de transferência, latência e desempenho, número de amostras coletadas e 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 período de coleta (em horas) são retornados.

Verbo HTTP	Caminho	Descrição
GET	/datacenter/storage/aggregates/{key}/metrics	Recupera dados de desempenho (amostra e resumo) para um agregado especificado pelo parâmetro de entrada da chave de agregação. Informações como intervalo de tempo, resumo do IOPS, latência, taxa de transferência e capacidade de desempenho, número de amostras coletadas para cada contador e 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 agregadas e de cluster, e valores, como IOPS agregado, taxa de transferência e 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 do LUN ou da chave de volume. Informações como o resumo do mínimo, máximo e média de IOPS de leitura, gravação e total, latência e taxa de transferência, além do 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 armazenamento, e valores, como IOPS agregado, taxa de transferência e período de coleta (em horas) são retornados.

Verbo HTTP	Caminho	Descrição
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 da VM de armazenamento. Resumo do IOPS com base em cada protocolo suportado, como <code>nvmf</code> , <code>fcp</code> , <code>iscsi</code> , <code>enfs</code> , a taxa de transferência, a 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 da VM de armazenamento, IOPS agregados, latência, taxa de transferência e período de coleta (em horas) são retornadas.
GET	/datacenter/network/ethernet/ports/{key}/metrics	Recupera as métricas de desempenho para uma porta Ethernet específica especificada pelo parâmetro de entrada da chave da 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 ao longo do 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 no seu ambiente de data center. Informações como chave do cluster e do nó, 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 do cluster e do nó, UUID e assim por diante.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Recupera as métricas de desempenho para 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 ao longo do período de tempo.
GET	/datacenter/network/fc/interfaces/analytics	Recupera as métricas de desempenho de alto nível para todas as portas Ethernet no seu ambiente de data center. Informações como o cluster e a chave da interface FC e UUID, taxa de transferência, IOPS, latência e VM de armazenamento são retornadas. Você pode filtrar o resultado pelos parâmetros disponíveis, como o nome e o UUID da interface do cluster e do FC, VM de armazenamento, taxa de transferência e assim por diante.

Verbo HTTP	Caminho	Descrição
GET	/datacenter/network/fc/ports/{key}/metrics	Recupera as métricas de desempenho para uma porta FC específica especificada pelo parâmetro de entrada da chave da 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 ao longo do período de tempo.
GET	/datacenter/network/fc/ports/analytics	Recupera as métricas de desempenho de alto nível para todas as portas FC no seu ambiente de data center. Informações como chave do cluster e do nó, 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 do cluster e do nó, UUID e assim por diante.
GET	/datacenter/network/ip/interfaces/{key}/metrics	Recupera as métricas de desempenho para uma interface IP de rede, conforme especificado pelo parâmetro de entrada da chave da 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 no seu ambiente de data center. Informações como o cluster e a chave da interface IP e UUID, taxa de transferência, IOPS e latência são retornadas. Você pode filtrar o resultado pelos parâmetros disponíveis, como o nome do cluster e da interface IP, UUID, IOPS, latência, taxa de transferência e assim por diante.

Ver trabalhos e detalhes do sistema

Você pode usar o `jobs` API sob o `management-server` categoria para visualizar os detalhes de execução de operações assíncronas. O `system` API sob o `management-server` A categoria permite que você visualize os detalhes da instância no seu ambiente do Active IQ Unified Manager .

Ver empregos

No Active IQ Unified Manager, operações como adicionar e modificar recursos são executadas por invocações de API síncronas e assíncronas. Invocações agendadas para execução assíncrona podem ser rastreadas por um objeto Job criado para essa invocação. Cada objeto Job tem uma chave exclusiva para identificação. Cada objeto Job retorna o URI do objeto Job para você acessar e acompanhar o progresso do trabalho. Você pode usar esta API para recuperar os detalhes de cada execução.

Ao usar esta API, você pode consultar todos os objetos Job do seu data center, incluindo dados históricos. Consultar todos os trabalhos, por padrão, retorna os detalhes dos últimos 20 trabalhos acionados por meio da interface da Web e da API. Use os filtros integrados para visualizar trabalhos específicos. Você também pode usar a chave Job para consultar os detalhes de um trabalho específico e executar o próximo conjunto de operações nos recursos.

Categoria	verbo HTTP	Caminho	Descrição
servidor de gerenciamento	PEGAR	/management-server/jobs	Retorna os detalhes de todos os trabalhos. Sem nenhuma ordem de classificação, o último objeto Job enviado é retornado no topo.

Categoria	verbo HTTP	Caminho	Descrição
servidor de gerenciamento	PEGAR	/management-server/jobs/{key} Insira a chave de trabalho do objeto Trabalho para visualizar os detalhes específicos desse trabalho.	Retorna os detalhes do objeto Job específico.

Ver detalhes do sistema

Ao usar o `/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 seu sistema, UUID, nome do fornecedor, sistema operacional do host e o nome, a descrição e o status dos serviços em execução na instância do Unified Manager.

Categoria	verbo HTTP	Caminho	Descrição
servidor de gerenciamento	PEGAR	/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.

Gerencie eventos e alertas usando APIs

O `events`, `alerts`, e `scripts` APIs sob o `management-server` categoria permite que você gerencie os eventos, alertas e scripts associados aos alertas no seu ambiente do Active IQ Unified Manager .

Ver e modificar eventos

O Unified Manager recebe os eventos gerados no ONTAP para os clusters monitorados e gerenciados pelo Unified Manager. Ao usar essas APIs, você pode visualizar os eventos gerados para seus clusters, resolvê-los e atualizá-los.

Ao executar o `GET` método para o `/management-server/events` API, você pode consultar os eventos no seu data center, incluindo dados históricos. Use os filtros incorporados, como nome, nível de impacto, área de impacto, gravidade, estado, nome do recurso e tipo de recurso, para visualizar eventos específicos. Os parâmetros de tipo de recurso e área retornam informações sobre o objeto de armazenamento no qual o evento ocorreu, e a área de impacto 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 `PATCH` para esta API, você pode habilitar 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 esta API para marcar o evento como resolvido.

Para mais informações sobre eventos, consulte ["Gerenciar eventos"](#) .

Categoria	verbo HTTP	Caminho	Descrição
servidor de gerenciamento	PEGAR	/management-server/events /management-server/events/{key}	Quando você executa o método Get ALL, o corpo da resposta consiste nos detalhes de todos os eventos no seu data center. Ao recuperar os detalhes do evento por uma chave específica, você pode visualizar os detalhes de um evento específico e executar o próximo conjunto de operações nos recursos. O corpo da resposta consiste nos detalhes desse evento.
servidor de gerenciamento	CORREÇÃO	management-server/events/{key}	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.

Gerenciar alertas

Os eventos são gerados automática 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. Ao usar o /management-server/alerts API, você pode configurar alertas para enviar notificações automaticamente quando eventos específicos ou eventos de certos tipos de gravidade ocorrerem.

Para obter mais informações sobre alertas, consulte ["Gerenciar alertas"](#) .

Categoria	verbo HTTP	Caminho	Descrição
servidor de gerenciamento	PEGAR	/management-server/alerts /management-server/alerts/{key}	Consulte todos os alertas existentes no seu ambiente ou um alerta específico, usando a chave de alerta. Você pode visualizar as informações sobre os alertas gerados em seu ambiente, como a descrição do alerta, a ação, o ID de e-mail para o qual a notificação é enviada, o evento e a gravidade.
servidor de gerenciamento	PUBLICAR	/management-server/alerts	Este método permite adicionar alertas para eventos específicos. Você deve adicionar o nome do alerta, o recurso físico ou lógico, ou o evento no qual o alerta é aplicável, se o alerta está habilitado e se você está emitindo traps SNMP. Você pode adicionar detalhes adicionais para os quais deseja gerar o alerta, como a ação, o ID do e-mail de notificação, os detalhes do script, caso esteja adicionando um script de alerta, e assim por diante.
servidor de gerenciamento	PATCH e DELETE	management-server/events/{key}	Você pode usar esses métodos para modificar e excluir alertas específicos. Você pode modificar diferentes atributos, como descrição, nome e habilitar e desabilitar o alerta. Você pode excluir um alerta quando ele não for mais necessário.



Ao selecionar um recurso para adicionar um alerta, observe que selecionar 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 de todos os clusters, receberá alertas somente para eventos críticos do cluster. Você não receberá alertas para eventos críticos em nós, agregados e assim por diante.

Gerenciar scripts

Ao usar o `/management-server/scripts` API, você também pode associar um alerta a um script que é executado quando um alerta é disparado. 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 dispara um alerta, o script é executado. Você pode carregar scripts personalizados e testar sua execução quando um alerta for gerado. Você pode associar um alerta ao seu script para que ele seja executado quando um alerta for gerado para um evento no Unified Manager.

Para mais informações sobre scripts, consulte "[Gerenciar scripts](#)".

Categoria	verbo HTTP	Caminho	Descrição
servidor de gerenciamento	PEGAR	<code>/management-server/scripts</code>	Use esta API para consultar todos os scripts existentes em seu ambiente. Use o filtro padrão e ordene por operações para visualizar apenas scripts específicos.
servidor de gerenciamento	PUBLICAR	<code>/management-server/scripts</code>	Use esta API para adicionar uma descrição ao script e carregar o arquivo de script associado a um alerta.

Gerencie cargas de trabalho usando APIs

As APIs descritas aqui abrangem várias funções de administração de armazenamento, como visualizar cargas de trabalho de armazenamento, criar LUNs e compartilhamentos de arquivos, gerenciar níveis de serviço de desempenho e políticas de eficiência de armazenamento e atribuir políticas em cargas de trabalho de armazenamento.

Visualize cargas de trabalho de armazenamento usando APIs

As APIs listadas aqui permitem que você visualize uma lista consolidada de cargas de trabalho de armazenamento para todos os clusters ONTAP no seu data center. As APIs também fornecem uma visão resumida do número de cargas de trabalho de armazenamento provisionadas no seu ambiente do Active IQ Unified Manager e suas estatísticas de capacidade e desempenho (IOPS).

Exibir cargas de trabalho de armazenamento

Você pode usar o método a seguir para visualizar todas as cargas de trabalho de armazenamento em todos os clusters do seu data center. Para obter informações sobre como filtrar a resposta com base em colunas específicas, consulte a documentação de referência da API disponível na sua instância do Unified Manager.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/workloads

Exibir resumo das cargas de trabalho de armazenamento

Você pode usar o método a seguir para avaliar a capacidade usada, a capacidade disponível, o IOPS usado, o IOPS disponível e o número de cargas de trabalho de armazenamento gerenciadas por cada Nível de Serviço de Desempenho. As cargas de trabalho de armazenamento exibidas podem ser para qualquer LUN, compartilhamento de arquivos NFS ou compartilhamento CIFS. A API fornece uma visão geral das cargas de trabalho de armazenamento, uma visão geral das cargas de trabalho de armazenamento provisionadas 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 dos Níveis de Serviço de Desempenho atribuídos. As informações recebidas em resposta a esta API são usadas para preencher o painel na interface do usuário do Unified Manager.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/workloads-summary

Gerenciar endpoints de acesso usando APIs

Você precisa criar pontos de extremidade de acesso ou interfaces lógicas (LIFs), que são necessários para provisionar máquinas virtuais de armazenamento (SVMs), LUNs e compartilhamentos de arquivos. Você pode visualizar, criar, modificar e excluir os pontos de extremidade de acesso para SVMs, LUNs ou compartilhamentos de arquivos no seu ambiente do Active IQ Unified Manager .

Exibir pontos de extremidade de acesso

Você pode visualizar uma lista dos pontos de extremidade de acesso no seu ambiente do Unified Manager usando o seguinte método. Para consultar uma lista de pontos de extremidade de acesso de um SVM, LUN ou compartilhamento de arquivos específico, você precisa inserir o identificador exclusivo do SVM, LUN ou compartilhamento de arquivos. Você também pode inserir a chave exclusiva do ponto de extremidade de acesso para recuperar os detalhes do ponto de extremidade de acesso específico.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/access-endpoints
		/storage-provider/access-endpoints/{key}

Adicionar pontos de extremidade de acesso

Você pode criar pontos de extremidade de acesso personalizados e atribuir propriedades necessárias a eles. Você deve inserir os detalhes do ponto de extremidade de acesso que deseja criar como parâmetros de entrada. Você pode usar esta API, o System Manager ou o ONTAP CLI para criar um ponto de extremidade de acesso em cada nó. Endereços IPv4 e IPv6 são suportados para criação de pontos de extremidade de acesso.



Você deve configurar seu 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 seu SVM com pelo menos dois pontos de extremidade de acesso por nó, um compatível com o protocolo CIFS e/ou NFS e outro compatível com o protocolo iSCSI ou FCP.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	/storage-provider/access-endpoints

Excluir pontos de extremidade de acesso

Você pode excluir um ponto de extremidade de acesso específico usando o seguinte método. Você precisa fornecer a chave do ponto de extremidade de acesso como um parâmetro de entrada para excluir um ponto de extremidade de acesso específico.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	EXCLUIR	/storage-provider/access-endpoints/{key}

Modificar pontos de extremidade de acesso

Você pode modificar um ponto de extremidade de acesso e atualizar suas propriedades usando o seguinte método. Você precisa fornecer a chave do ponto de extremidade de acesso para modificar um ponto de extremidade de acesso específico. Você também precisa inserir a propriedade que deseja atualizar, juntamente com seu valor.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	CORREÇÃO	/storage-provider/access-endpoints/{key}

Gerenciar mapeamento do Active Directory usando APIs

Você pode usar as APIs listadas aqui para gerenciar mapeamentos do Active Directory no SVM que são necessários para provisionar compartilhamentos CIFS nos SVMs. Os mapeamentos do Active Directory precisam ser configurados para mapear as SVMs com o ONTAP.

Exibir mapeamentos do Active Directory

Você pode visualizar os detalhes de configuração dos mapeamentos do Active Directory para uma SVM usando o seguinte método. Para visualizar os mapeamentos do Active Directory em uma SVM, você precisa inserir a chave SVM. Para consultar os detalhes de um mapeamento específico, você deve inserir a chave de mapeamento.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	<code>/storage-provider/active-directories-mappings</code> <code>/storage-provider/active-directories-mappings/{key}</code>

Adicionar mapeamento do Active Directory

Você pode criar mapeamentos do Active Directory em uma SVM usando o seguinte método. Você deve inserir os detalhes do mapeamento como parâmetros de entrada.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	<code>/storage-provider/active-directories-mappings</code>

Gerenciar compartilhamentos de arquivos usando APIs

Você pode usar o `/storage-provider/file-shares` API para visualizar, adicionar, modificar e excluir os volumes de compartilhamento de arquivos CIFS e NFS no seu ambiente de data center.

Antes de provisionar os volumes de compartilhamento de arquivos, certifique-se de que o SVM tenha sido criado e provisionado com os protocolos suportados. Se você estiver atribuindo Níveis de Serviço de Desempenho (PSLs) ou Políticas de Eficiência de Armazenamento (SEPs), durante o provisionamento, os PSLs ou SEPs deverão ser criados antes de criar os compartilhamentos de arquivos.

Ver compartilhamentos de arquivos

Você pode usar o método a seguir para visualizar os volumes de compartilhamento de arquivos disponíveis no seu ambiente do Unified Manager. Quando você adiciona um cluster ONTAP como uma fonte de dados no Active IQ Unified Manager, as cargas de trabalho de armazenamento para esses clusters são adicionadas automaticamente à sua instância do Unified Manager. Esta API recupera os compartilhamentos de arquivos automaticamente e os adiciona manualmente à sua instância do Unified Manager. Você pode visualizar os detalhes de um compartilhamento de arquivo específico executando esta API com a chave de compartilhamento de arquivo.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/file-shares /storage-provider/file-shares/{key}

Adicionar compartilhamentos de arquivos

Você pode usar o seguinte método para adicionar compartilhamentos de arquivos CIFS e NFS no seu SVM. Você deve inserir os detalhes do compartilhamento de arquivos que deseja criar como parâmetros de entrada. Você não pode usar esta API para adicionar volumes FlexGroup .

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	/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 da ACL, os compartilhamentos CIFS não serão criados e os compartilhamentos NFS serão criados por padrão, fornecendo acesso a todos.

Criando volumes de proteção de dados: Quando você adiciona compartilhamentos de arquivos ao seu SVM, o tipo de volume que é montado, por padrão, é `rw` (leitura-escrita). Para criar volumes de proteção de dados (DP), especifique `dp` como o valor para o `type` parâmetro.

Excluir compartilhamentos de arquivos

Você pode usar o seguinte método para excluir um compartilhamento de arquivo específico. Você precisa inserir a chave de compartilhamento de arquivos como um parâmetro de entrada para excluir um compartilhamento de arquivo específico.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	EXCLUIR	/storage-provider/file-shares/{key}

Modificar compartilhamentos de arquivos

Você pode usar o seguinte método para modificar um compartilhamento de arquivos e atualizar suas propriedades.

Você precisa fornecer a chave de compartilhamento de arquivos para modificar um compartilhamento de arquivos específico. Além disso, você precisa inserir o imóvel que deseja atualizar, juntamente com seu valor.



Observe que você pode atualizar apenas uma propriedade em uma única invocação desta API. Para múltiplas atualizações, você precisa executar esta API quantas vezes quiser.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	CORREÇÃO	/storage-provider/file-shares/{key}

Gerenciar LUNs usando APIs

Você pode usar o `/storage-provider/luns` API para visualizar, adicionar, modificar e excluir LUNs no seu ambiente de data center.

Antes de provisionar os LUNs, certifique-se de que o SVM tenha sido criado e provisionado com os protocolos suportados. Se você estiver atribuindo Níveis de Serviço de Desempenho (PSLs) ou Políticas de Eficiência de Armazenamento (SEPs), durante o provisionamento, os PSLs ou SEPs deverão ser criados antes de criar o LUN.

Exibir LUNs

Você pode usar o seguinte método para visualizar os LUNs no seu ambiente do Unified Manager. Quando você adiciona um cluster ONTAP como uma fonte de dados no Active IQ Unified Manager, as cargas de trabalho de armazenamento para esses clusters são adicionadas automaticamente à sua instância do Unified Manager. Esta API recupera todos os LUNs automaticamente e os adiciona manualmente à sua instância do Unified Manager. Você pode visualizar os detalhes de um LUN específico executando esta API com a chave LUN.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/luns /storage-provider/luns/{key}

Adicionar LUNs

Você pode usar o seguinte método para adicionar LUNs às suas SVMs.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	/storage-provider/luns



Na 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 do LUN. Esta tag permite pesquisar o volume facilmente. Se você fornecer a chave de volume na solicitação, a marcação será ignorada.

Excluir 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 então provisionado LUNs por meio do Unified Manager nesse volume, quando você excluir todos os LUNs usando esta API, o volume também será excluído do cluster ONTAP .

Categoria	verbo HTTP	Caminho
provedor de armazenamento	EXCLUIR	/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 matrizes LUN usando esta 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 múltiplas atualizações, você precisa executar esta API quantas vezes quiser.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	CORREÇÃO	/storage-provider/luns/{key}

Gerencie os níveis de serviço de desempenho usando APIs

Você pode visualizar, criar, modificar e excluir Níveis de Serviço de Desempenho usando as APIs do provedor de armazenamento no seu Active IQ Unified Manager.

Ver níveis de serviço de desempenho

Você pode usar o método a seguir para visualizar os Níveis de Serviço de Desempenho para atribuí-los às cargas de trabalho de armazenamento. 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 quiser consultar um Nível de Serviço de Desempenho específico, você precisa inserir o ID exclusivo do Nível de Serviço de Desempenho para recuperar seus detalhes.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/performance-service-levels /storage-provider/performance-service-levels/{key}

Adicionar níveis de serviço de desempenho

Você pode usar o método a seguir para criar Níveis de Serviço de Desempenho personalizados e atribuí-los às suas cargas de trabalho de armazenamento se os Níveis de Serviço de Desempenho definidos pelo sistema não atenderem aos objetivos de nível de serviço (SLOs) necessários para as cargas de trabalho de armazenamento. Insira os detalhes do Nível de Serviço de Desempenho que você deseja criar. Para as propriedades do IOPS, certifique-se de inserir um intervalo válido de valores.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	/storage-provider/performance-service-levels

Excluir 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 estiver 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.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	EXCLUIR	/storage-provider/performance-service-levels/{key}

Modificar os 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 Desempenho 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.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	CORREÇÃO	/storage-provider/performance-service-levels/{key}

Visualizar recursos agregados com base nos níveis de serviço de desempenho

Você pode usar o método a seguir para consultar os recursos agregados com base nos Níveis de Serviço de Desempenho. Esta API retorna a lista de agregados disponíveis no seu data center e indica os recursos em termos de Níveis de Serviço de Desempenho que podem ser suportados nesses agregados. Ao provisionar cargas de trabalho em um volume, você pode visualizar a capacidade de um agregado de oferecer suporte a um Nível de Serviço de Desempenho específico e provisionar cargas de trabalho com base nessa capacidade. Sua capacidade de especificar o agregado está disponível somente quando você provisiona uma carga de trabalho usando APIs. Esta funcionalidade não está disponível na interface web do Unified Manager.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/aggregate-capabilities /storage-provider/aggregate-capabilities/{key}

Gerencie políticas de eficiência de armazenamento usando APIs

Você pode visualizar, criar, modificar e excluir Políticas de Eficiência de Armazenamento usando as APIs do provedor de armazenamento.

Observe os seguintes pontos:



- Não é obrigatório atribuir uma Política de Eficiência de Armazenamento ao criar uma carga de trabalho no Unified Manager.
- Não é possível cancelar a atribuição de uma Política de Eficiência de Armazenamento de uma carga de trabalho depois que uma política é atribuída a ela.
- Se uma carga de trabalho tiver algumas configurações de armazenamento especificadas em volumes ONTAP , como desduplicação e compactação, essas configurações poderão ser substituídas pelas configurações especificadas na Política de Eficiência de Armazenamento que você aplica ao adicionar as cargas de trabalho de armazenamento no Unified Manager.

Ver políticas de eficiência de armazenamento

Você pode usar o método a seguir para visualizar as Políticas de Eficiência de Armazenamento antes de atribuí-las às cargas de trabalho de armazenamento. 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 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 armazenamento	PEGAR	/storage-provider/storage-efficiency-policies /storage-provider/storage-efficiency-policies/{key}

Adicionar políticas de eficiência de armazenamento

Você pode usar o método a seguir para criar Políticas de Eficiência de Armazenamento personalizadas e atribuí-las às suas cargas de trabalho de armazenamento se as políticas definidas pelo sistema não atenderem aos requisitos de provisionamento para suas cargas de trabalho de armazenamento. Insira os detalhes da Política de Eficiência de Armazenamento que você deseja criar, como parâmetros de entrada.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	/storage-provider/storage-efficiency-policies

Excluir políticas de eficiência de armazenamento

Você pode usar o seguinte método para excluir uma Política de Eficiência de Armazenamento específica. Não é possível excluir uma Política de Eficiência de Armazenamento se ela estiver atribuída a uma carga de trabalho ou se for a única Política de Eficiência de Armazenamento 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.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	EXCLUIR	/storage-provider/storage-efficiency-policies/{key}

Modificar políticas de eficiência de armazenamento

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 Armazenamento definida pelo sistema ou atribuída a uma carga de trabalho. Você precisa fornecer o ID exclusivo da Política de Eficiência de Armazenamento para modificar uma Política de Eficiência de Armazenamento específica. Além disso, você precisa fornecer a propriedade que deseja atualizar, juntamente com seu valor.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	CORREÇÃO	/storage-provider/storage-efficiency-policies/{key}

Fluxos de trabalho de API comuns para gerenciamento de armazenamento

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 armazenamento. Esta seção contém alguns desses fluxos de trabalho de exemplo.

Os fluxos de trabalho descrevem alguns dos casos de uso de gerenciamento de armazenamento mais 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.

Entenda as chamadas de API usadas nos fluxos de trabalho

Você pode visualizar a página de documentação on-line da sua instância do Unified Manager que inclui os detalhes de cada chamada da 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. Após 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 da solicitação.

As seguintes informações são incluídas para cada chamada de API em 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 o final da página e clique na categoria de API aplicável.
- **Verbo HTTP (chamar):** O verbo HTTP identifica a ação realizada em um recurso. Cada chamada de API é executada por meio 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 string do caminho é anexada à URL principal para formar a URL completa que identifica o recurso.

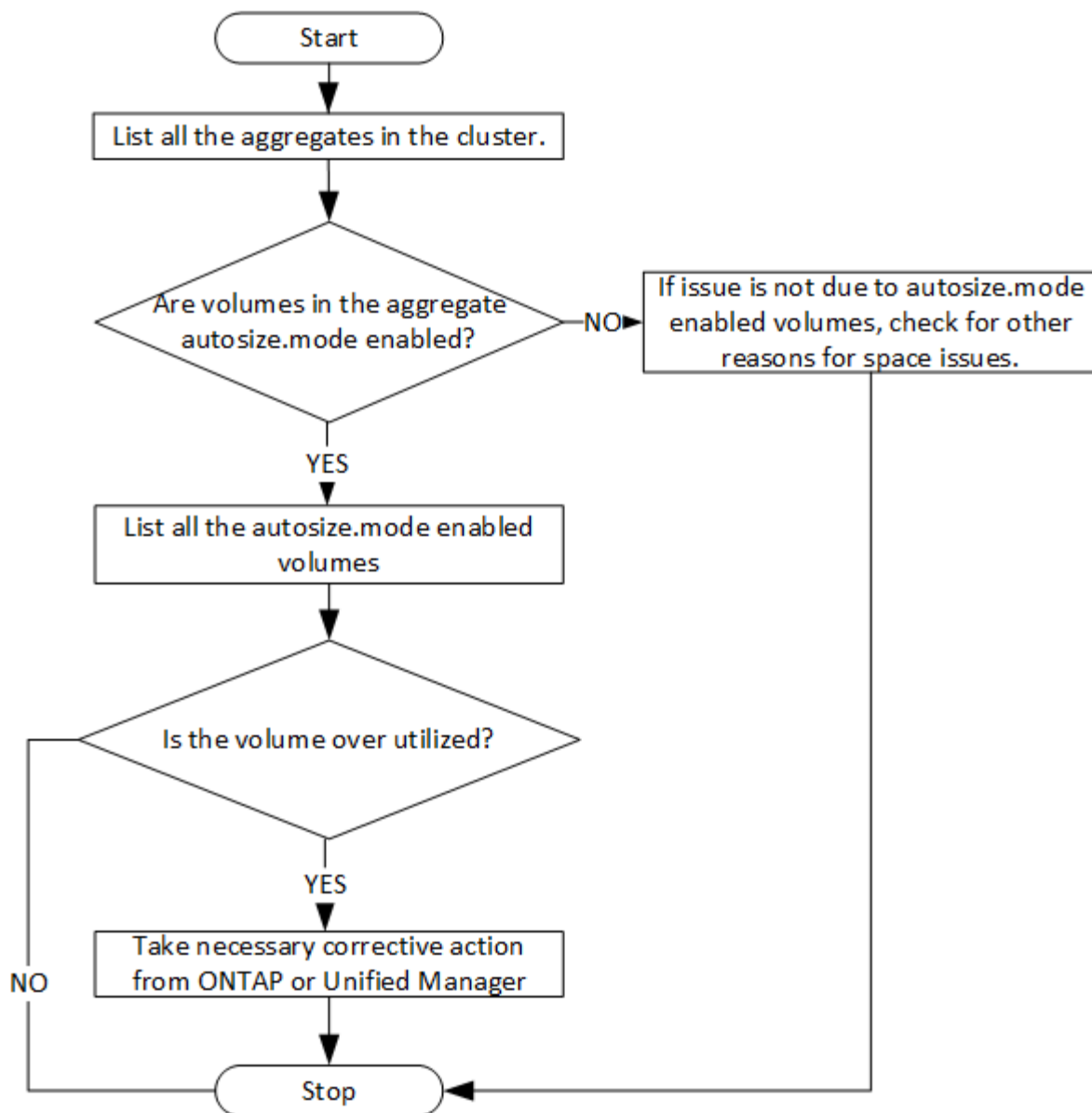
Determinar problemas de espaço em agregados usando APIs

Você pode usar as APIs do data center no Active IQ Unified Manager para monitorar a disponibilidade e a utilização de espaço em seus volumes. Você pode determinar problemas de espaço no seu volume e identificar recursos de armazenamento que estão sendo superutilizados ou subutilizados.

As APIs do data center para agregados recuperam informações relevantes sobre o espaço disponível e usado, além de configurações de eficiência para economia de espaço. Você também pode filtrar as informações recuperadas com base em atributos especificados.

Um método para determinar qualquer falta de espaço em seus agregados é verificar se há volumes em seu ambiente com o modo de dimensionamento automático habilitado. Você deve então identificar quais volumes estão sendo utilizados em excesso e executar quaisquer ações corretivas.

O fluxograma a seguir ilustra o processo de recuperação de informações sobre volumes com o modo de dimensionamento automático habilitado:



Este fluxo pressupõe que os clusters já foram criados no ONTAP e adicionados ao Unified Manager.

1. Obtenha a chave do cluster, a menos que você saiba o valor:

Categoria	verbo HTTP	Caminho
centro de dados	PEGAR	/datacenter/cluster/clusters

2. Usando a chave do cluster como parâmetro de filtro, consulte os agregados nesse cluster.

Categoria	verbo HTTP	Caminho
centro de dados	PEGAR	/datacenter/storage/aggregates

3. A partir da resposta, analise o uso de espaço dos agregados e determine quais agregados têm problemas de espaço. Para cada agregado com problema de espaço, obtenha a chave de agregação da mesma saída JSON.
4. Usando cada chave agregada, filtre todos os volumes que têm o valor para o parâmetro `autosize.mode` como `grow`.

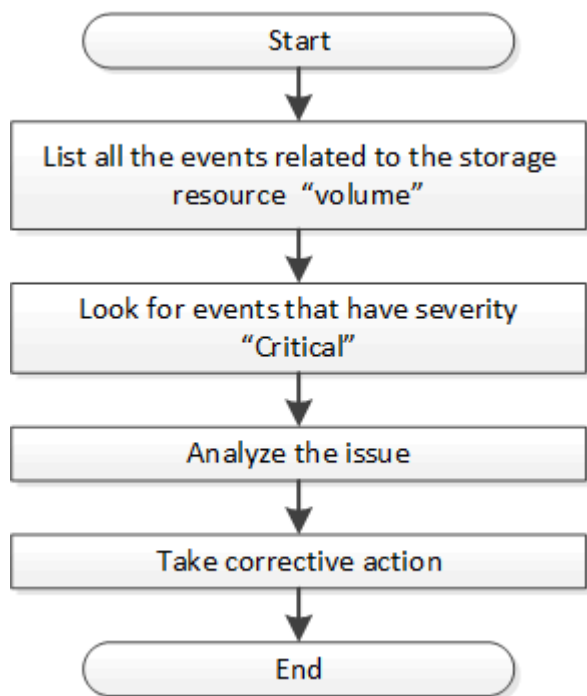
Categoria	verbo HTTP	Caminho
centro de dados	PEGAR	/datacenter/storage/volumes

5. Analise quais volumes estão sendo superutilizados.
6. Execute qualquer ação corretiva necessária, como mover o volume entre agregados, para resolver os problemas de espaço no seu volume. Você pode executar essas ações no ONTAP ou na interface da Web do Unified Manager.

Determinar problemas em objetos de armazenamento usando APIs de eventos

Quando um objeto de armazenamento no seu data center ultrapassa um limite, você recebe uma notificação sobre esse evento. Usando esta notificação, você pode analisar o problema e tomar medidas corretivas usando o `events` APIs.

Este fluxo de trabalho usa o exemplo de um volume como objeto de recurso. Você pode usar o `events` APIs para recuperar a lista de eventos relacionados a um volume, analisar os problemas críticos desse volume e, em seguida, tomar ações corretivas para corrigir o problema.



Siga estas etapas para determinar os problemas no seu volume antes de tomar medidas corretivas.

Passos

1. Analise as notificações de eventos críticos do Active IQ Unified Manager para os volumes no seu data

center.

2. Consulte todos os eventos dos volumes usando os seguintes parâmetros na API /management-server/events:

```
"resource_type": "volume"
"severity": "critical"
```

Categoria	verbo HTTP	Caminho
servidor de gerenciamento	PEGAR	/servidor-de-gerenciamento/eventos

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 interface de usuário da Web para resolver os problemas.

Solucionar problemas de volumes ONTAP usando APIs de gateway

As APIs de gateway atuam como um gateway para invocar APIs ONTAP para consultar informações sobre seus objetos de armazenamento ONTAP e tomar medidas corretivas para resolver os problemas relatados.

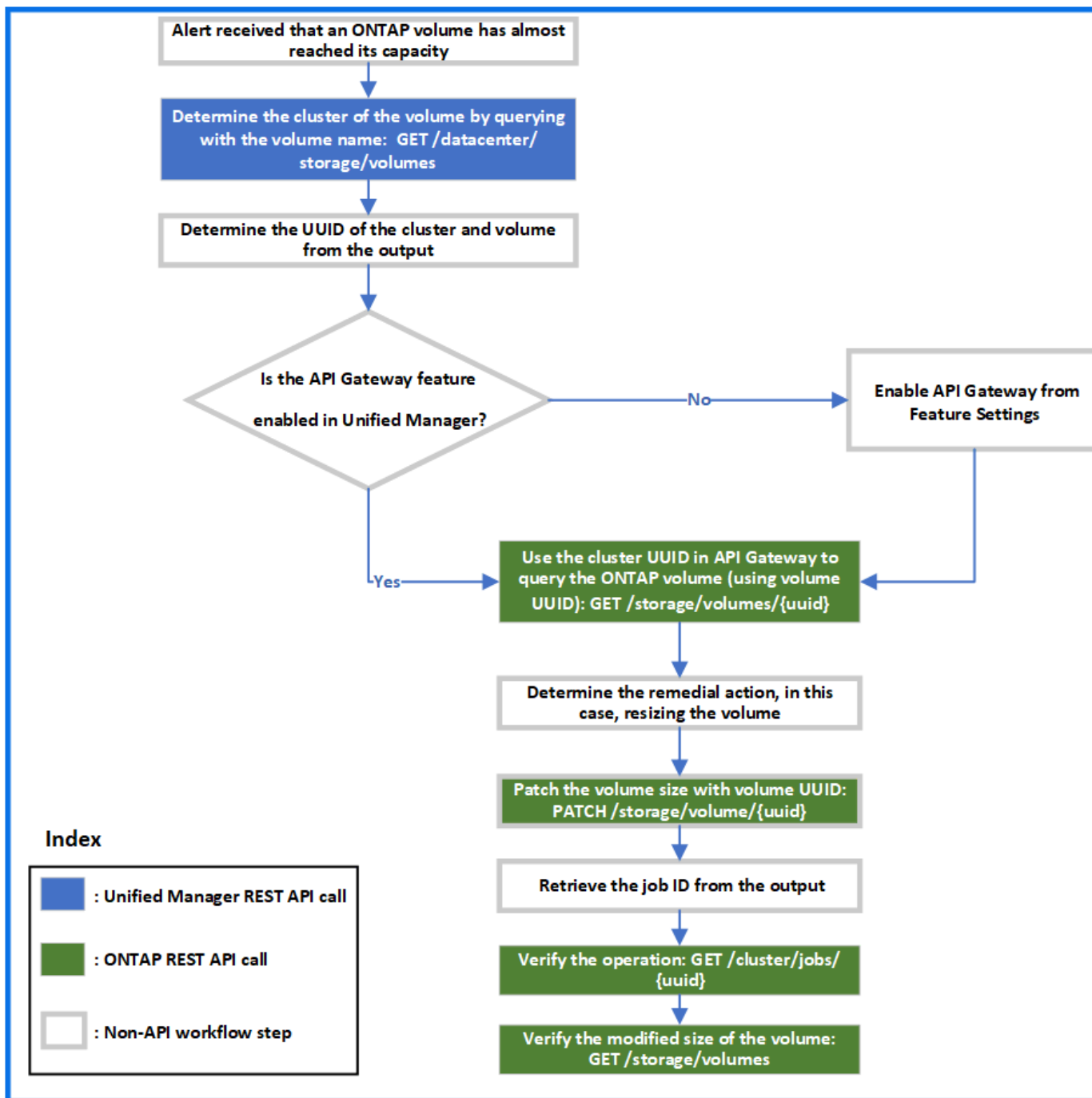
Este fluxo de trabalho utiliza um caso de uso de exemplo no qual um evento é gerado quando um volume ONTAP quase atinge sua capacidade. O fluxo de trabalho também demonstra como resolver esse problema invocando uma combinação de APIs REST do Active IQ Unified Manager e do ONTAP .

Antes de executar as etapas do fluxo de trabalho, certifique-se do seguinte:



- Você conhece as APIs de gateway e como elas são usadas. Para obter informações, consulte ["Acessando APIs ONTAP por meio de acesso proxy"](#) .
- Você está ciente do uso das APIs REST do ONTAP . Para obter informações sobre o uso de APIs REST do ONTAP , consulte <https://docs.netapp.com/us-en/ontap-automation/index.html> ["Documentação de automação ONTAP"] .
- 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 por HTTPS.

O diagrama a seguir ilustra cada etapa do fluxo de trabalho para solucionar o problema de uso da capacidade do volume 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 que notifica a utilização da capacidade do volume.
2. Usando o nome do volume como valor no parâmetro name, consulte o volume executando a seguinte API do Unified Manager.

Categoria	verbo HTTP	Caminho
centro de dados	PEGAR	/datacenter/storage/volumes

3. Recupere o UUID do cluster e o UUID do volume da saída.

- Na interface da Web do Unified Manager, navegue até **Geral > Configurações de recursos > API Gateway** para verificar se o recurso API Gateway está habilitado. A menos que esteja habilitado, as APIs na categoria gateway não estarão disponíveis para você invocar. Habilite o recurso se ele estiver desabilitado.
- Use o UUID do cluster para executar a API ONTAP/`storage/volumes/{uuid}` através do gateway de API. A consulta retorna os detalhes do volume quando o UUID do volume é passado como parâmetro da API.

Para executar as APIs do ONTAP por meio do gateway de API, as credenciais do Unified Manager são passadas internamente para autenticação, e você não precisa executar uma etapa de autenticação adicional para acesso individual ao cluster.

Categoria	verbo HTTP	Caminho
Gerenciador unificado: gateway	PEGAR	API de gateway: <code>/gateways/{uuid}/{path}</code>
ONTAP: armazenamento		API ONTAP : <code>/storage/volumes/{uuid}</code>



Em `/gateways/{uuid}/{path}`, o valor de `{uuid}` deve ser substituído pelo UUID do cluster no qual a operação REST deve ser executada. `{path}` deve ser substituído pelo URL REST do ONTAP `/storage/volumes/{uuid}`.

O URL anexado é: `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

Ao executar a operação GET, a URL gerada é:

`GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes/{volume_uuid}`

Exemplo de comando cURL

```
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>"
```

- A partir da saída, determine o tamanho, o uso e as medidas corretivas a serem tomadas. Neste fluxo de trabalho, a medida corretiva tomada é redimensionar o volume.
- Use o UUID do cluster e execute a seguinte API ONTAP por meio do gateway de API para redimensionar o volume. Para obter informações sobre os parâmetros de entrada para as APIs do gateway e do ONTAP, consulte a etapa 5.

Categoria	verbo HTTP	Caminho
Gerenciador unificado: gateway ONTAP: armazenamento	CORREÇÃO	API de gateway: /gateways/{uuid}/{path} API ONTAP : /storage/volumes/{uuid}



Junto com o UUID do cluster e o UUID do volume, você deve inserir um valor para o parâmetro de 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, insira o valor do parâmetro size no final da consulta: `-d {"size": 128849018880}`

Exemplo de comando cURL

```
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.

- Verifique se o trabalho foi executado com sucesso usando o UUID do trabalho. Use o UUID do cluster e o UUID do trabalho para executar a seguinte API ONTAP por meio do gateway de API. Para obter informações sobre os parâmetros de entrada para as APIs do gateway e do ONTAP , consulte a etapa 5.

Categoria	verbo HTTP	Caminho
Gerenciador unificado: gateway ONTAP: cluster	PEGAR	API de gateway: /gateways/{uuid}/{path} API ONTAP : /cluster/jobs/{uuid}

Os códigos HTTP retornados são os mesmos que os códigos de status HTTP da API REST do ONTAP .

- Execute a seguinte API ONTAP para consultar os detalhes do volume redimensionado. Para obter informações sobre os parâmetros de entrada para as APIs do gateway e do ONTAP , consulte a etapa 5.

Categoria	verbo HTTP	Caminho
Gerenciador unificado: gateway ONTAP: armazenamento	PEGAR	API de gateway: /gateways/{uuid}/{path} API ONTAP : /storage/volumes/{uuid}

A saída exibe um tamanho de volume aumentado de 120 GB.

Fluxos de trabalho de API para gerenciamento de carga de trabalho

Usando o Active IQ Unified Manager, você pode provisionar e modificar cargas de trabalho de armazenamento (LUNs, compartilhamentos de arquivos NFS e compartilhamentos CIFS). O provisionamento consiste em várias etapas, desde a criação da Máquina Virtual de Armazenamento (SVM) até a aplicação de Políticas de Nível de Serviço de Desempenho e Eficiência de Armazenamento nas cargas de trabalho de armazenamento. 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 provisionamento de máquinas virtuais de armazenamento (SVMs) no Unified Manager.



esse fluxo de trabalho deve ser executado antes do provisionamento de LUNs ou compartilhamentos de arquivos no Unified Manager.

- Provisionando compartilhamentos de arquivos.
- Provisionando LUNs.
- Modificando LUNs e compartilhamentos de arquivos (usando o exemplo para atualizar o parâmetro Nível de Serviço de Desempenho para as cargas de trabalho de armazenamento).
- Modificando um compartilhamento de arquivo NFS para suportar o protocolo CIFS
- Modificando cargas de trabalho para atualizar QoS para AQoS



Para cada fluxo de trabalho de provisionamento (LUN e compartilhamentos de arquivos), certifique-se de ter concluído o fluxo de trabalho para verificar as 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.

Verifique 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 ONTAP foram adicionados ao Unified Manager e que a chave do cluster foi 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
centro de dados	PEGAR	/datacenter/svm/svms /datacenter/svm/svms/{key} }

Exemplo de cURL

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

- Se a chave SVM não for retornada, crie o SVM. Para criar as SVMs, você precisa da chave de cluster na qual provisiona a SVM. Você também precisa especificar o nome do SVM. Siga estes passos.

Categoria	verbo HTTP	Caminho
centro de dados	PEGAR	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}

Obtenha a chave do cluster.

Exemplo de cURL

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

- A partir da saída, obtenha a chave do cluster e use-a como entrada para criar o SVM.



Ao criar o SVM, certifique-se de que ele suporte todos os protocolos necessários para provisionar LUNs e compartilhamentos de arquivos neles, por exemplo, CIFS, NFS, FCP e iSCSI. Os fluxos de trabalho de provisionamento podem falhar se o SVM não oferecer suporte aos serviços necessários. É recomendável que os serviços para os respectivos tipos de cargas de trabalho também sejam habilitados no SVM.

Categoria	verbo HTTP	Caminho
centro de dados	PUBLICAR	/datacenter/svm/svms

Exemplo de cURL

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 do objeto de trabalho para consulta. Se o SVM for criado com sucesso, a chave SVM será retornada na resposta.

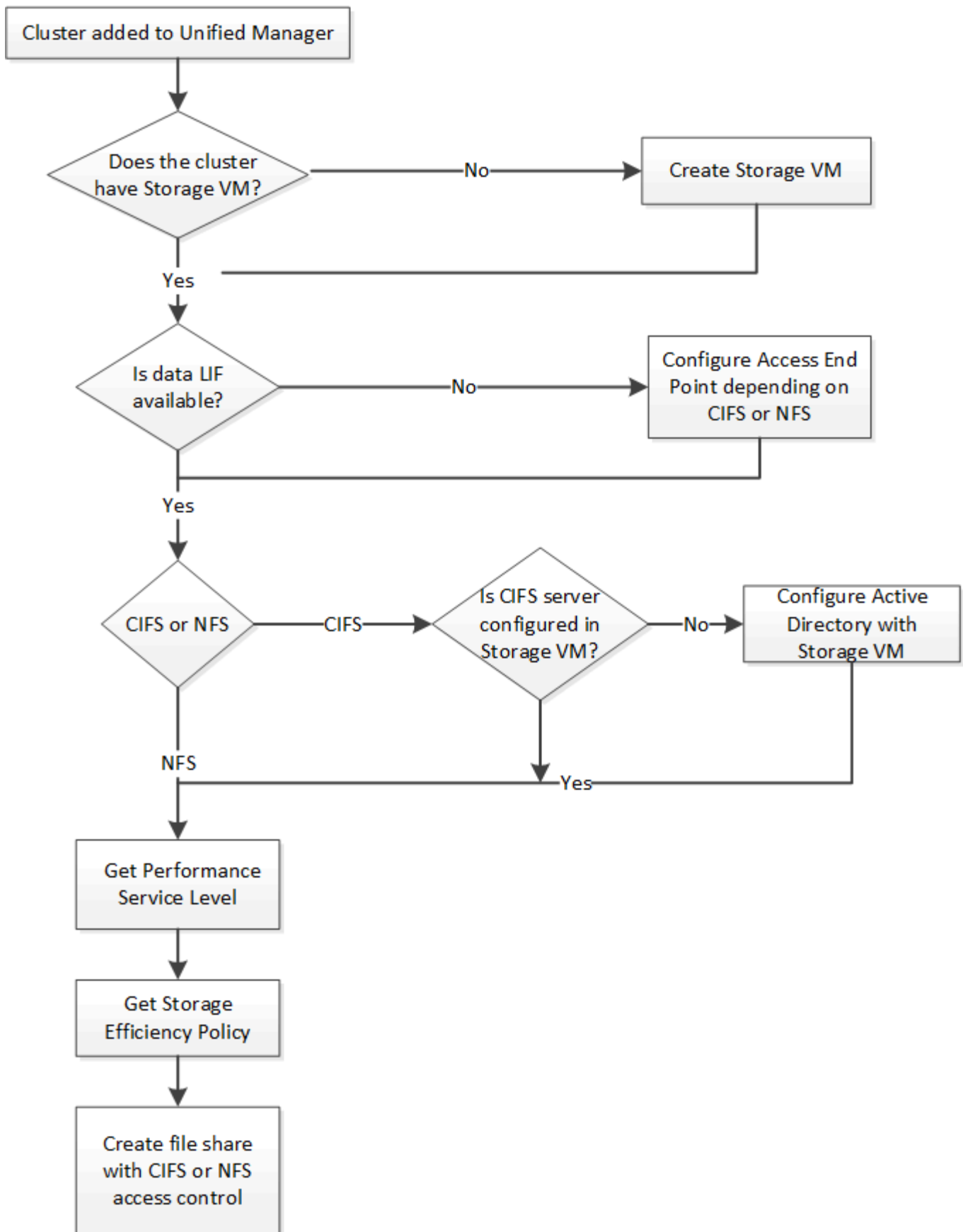
Categoria	verbo HTTP	Caminho
servidor de gerenciamento	PEGAR	/management-server/jobs/{key}

Provisionar compartilhamentos de arquivos CIFS e NFS usando APIs

Você pode provisionar compartilhamentos CIFS e compartilhamentos de arquivos NFS em suas Máquinas Virtuais de Armazenamento (SVMs) usando as APIs de

provisionamento fornecidas como parte do Active IQ Unified Manager. Este fluxo de trabalho de provisionamento detalha as etapas para recuperar as chaves dos SVMs, Níveis de Serviço de Desempenho e Políticas de Eficiência de Armazenamento antes de criar os compartilhamentos de arquivos.

O diagrama a seguir ilustra cada etapa em um fluxo de trabalho de provisionamento de compartilhamento de arquivos. Inclui o provisionamento de compartilhamentos CIFS e compartilhamentos de arquivos NFS.



Garanta o seguinte:



- Os clusters ONTAP foram adicionados ao Unified Manager e a chave do cluster foi obtida.
- SVMs foram criadas nos clusters.
- Os SVMs suportam serviços CIFS e NFS. O provisionamento de compartilhamentos de arquivos pode falhar se as SVMs não suportarem os serviços necessários.
- A porta FCP está online para provisionamento de porta.

1. Determine se os LIFs de dados ou os pontos de extremidade de acesso estão disponíveis no SVM no qual você deseja criar o compartilhamento CIFS. Obtenha a lista de pontos de extremidade de acesso disponíveis no SVM:

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

Exemplo de cURL

```
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 do ponto de extremidade de acesso; caso contrário, crie o ponto de extremidade de acesso.



Certifique-se de criar pontos de extremidade de acesso que tenham o protocolo CIFS habilitado. O provisionamento de compartilhamentos CIFS falha, a menos que você tenha criado um ponto de extremidade de acesso com o protocolo CIFS habilitado.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	/storage-provider/access-endpoints

Exemplo de cURL

Você deve inserir os detalhes do ponto de extremidade 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 ponto de extremidade de acesso que você criou.

3. Verifique o ponto de extremidade de acesso:

Categoria	verbo HTTP	Caminho
servidor de gerenciamento	PEGAR	/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:

- Determine se o servidor CIFS está configurado no seu SVM, ou seja, determine se um mapeamento do Active Directory foi criado no SVM.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/active-directories-mappings

- Se o mapeamento do Active Directory for criado, pegue a chave; caso contrário, crie o mapeamento do Active Directory no SVM.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	/storage-provider/active-directories-mappings

Exemplo de cURL

Você deve inserir os detalhes para criar o mapeamento do Active Directory como 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 será exibida para você solucionar o problema e executar a solicitação novamente.

- 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
provedor de armazenamento	PEGAR	/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 para `true`. Na saída, obtenha a chave do Nível de Serviço de Desempenho que você deseja aplicar no compartilhamento de arquivos.

- Opcionalmente, obtenha a chave da Política de Eficiência de Armazenamento que você deseja aplicar no compartilhamento de arquivos executando a seguinte API e recuperando a chave da resposta.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/storage-efficiency-policies

- 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 caso você queira criar um compartilhamento de arquivos para oferecer suporte a 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 *Modificando 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 atribuído, uma ACL é criada quando um compartilhamento CIFS/SMB é provisionado. Com base nos valores inseridos para o mapeamento de ACL e do Active 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 ele é criado.



Ao provisionar o compartilhamento NFS, você pode criar uma política de exportação fornecendo todos os valores necessários ou fornecer a chave da política de exportação e reutilizar uma política de exportação existente. Se quiser reutilizar uma política de exportação para a VM de armazenamento, você precisará adicionar a chave da política de exportação. A menos que você saiba a chave, você pode recuperar a chave da política de exportação usando o `/datacenter/protocols/nfs/export-policies` API. Para criar uma nova política, você deve inserir as regras conforme exibido no exemplo a seguir. Para as regras inseridas, a API tenta procurar uma política de exportação existente correspondendo ao host, à VM de armazenamento e às regras. Se houver uma política de exportação existente, ela será usada. Caso contrário, uma nova política de exportação será 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"
        }
      ]
    }
  ]
}
```

Após 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 Armazenamento é um parâmetro opcional para criar compartilhamentos de arquivos.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	/storage-provider/file-shares

A saída JSON exibe uma chave de objeto Job que você pode usar para verificar o compartilhamento de arquivos que você criou. . Verifique a criação do compartilhamento de arquivos usando a chave do objeto Job retornada na consulta do job:

Categoria	verbo HTTP	Caminho
servidor de gerenciamento	PEGAR	/management-server/jobs/{key}

No final da resposta, você vê a chave do compartilhamento de arquivo criado.

```

],
"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
provedor de armazenamento	PEGAR	/storage-provider/file-shares/{key}

Exemplo de saída JSON

Você pode ver que o método POST de /storage-provider/file-shares invoca internamente todas as APIs necessárias para cada uma das funções e cria o objeto. Por exemplo, invoca o /storage-provider/performance-service-levels/ API para atribuição do 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": [

```

```

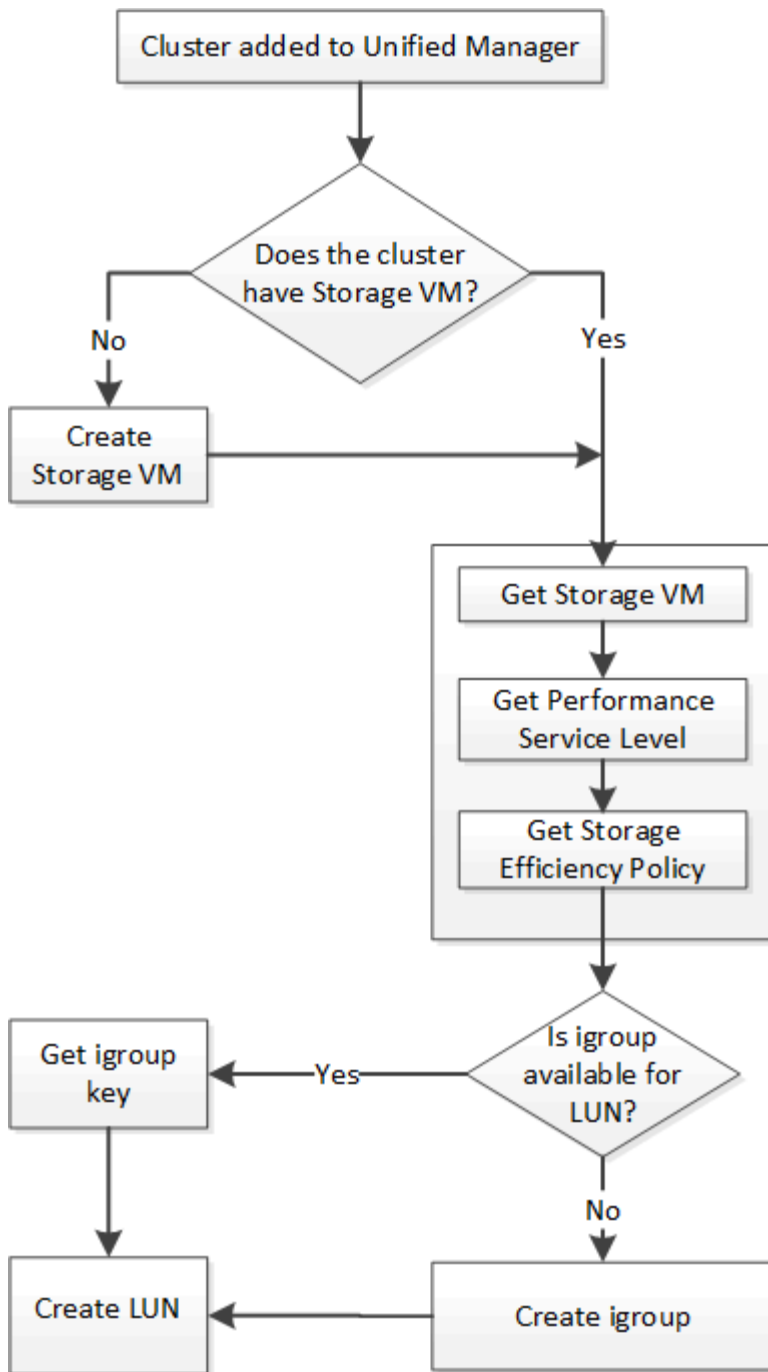
        "ntlm"
    ],
    "superuser": [
        "none"
    ]
}
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
},
"_links": {
    "self": {
        "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
    }
}
}
}

```

Provisionar LUNs usando APIs

Você pode provisionar LUNs em suas Máquinas Virtuais de Armazenamento (SVMs) usando as APIs de provisionamento fornecidas como parte do Active IQ Unified Manager. Este fluxo de trabalho de provisionamento detalha as etapas para recuperar as chaves dos SVMs, Níveis de Serviço de Desempenho e Políticas de Eficiência de Armazenamento antes de criar o LUN.

O diagrama a seguir ilustra as etapas em um fluxo de trabalho de provisionamento de LUN.



Este fluxo de trabalho pressupõe que os clusters ONTAP foram adicionados ao Unified Manager e que a chave do cluster foi obtida. O fluxo de trabalho também pressupõe que as SVMs já foram criadas nos clusters.

1. Obtenha a chave SVM para a SVM na qual você deseja criar o LUN, conforme descrito no tópico de fluxo de trabalho *Verificando SVMs em clusters*.
2. Obtenha a chave para o Nível de Serviço de Desempenho executando a seguinte API e recuperando a chave da resposta.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/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 para `true`. Na saída, obtenha a chave do Nível de Serviço de Desempenho que você deseja aplicar ao LUN.

3. Opcionalmente, obtenha a chave da 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.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/storage-efficiency-policies

4. Determine se grupos iniciadores (igroups) foram criados para conceder acesso ao destino LUN que você deseja criar.

Categoria	verbo HTTP	Caminho
centro de dados	PEGAR	/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 igroup específico, insira o nome do igroup (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 igroup.

Categoria	verbo HTTP	Caminho
centro de dados	PUBLICAR	/datacenter/protocols/san/igroups

Você deve inserir os detalhes do igroup que deseja criar como parâmetros de entrada. Esta é uma chamada síncrona e você pode verificar a criação do igroup na saída. Em caso de erro, uma mensagem será exibida para você solucionar o problema e executar novamente a API.

6. Crie o LUN.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	/storage-provider/luns

Para criar o LUN, certifique-se de ter adicionado os valores recuperados como parâmetros de entrada obrigatórios.



A Política de Eficiência de Armazenamento é um parâmetro opcional para criar LUNs.

Exemplo de cURL

Você deve inserir todos os detalhes do LUN que deseja criar, como parâmetros de entrada.

A saída JSON exibe uma chave de objeto Job que você pode usar para verificar o LUN criado.

7. Verifique a criação do LUN usando a chave do objeto Job retornada na consulta do Job:

Categoria	verbo HTTP	Caminho
servidor de gerenciamento	PEGAR	/management-server/jobs/{key}

No final da resposta, você vê a chave do LUN criado.

8. Verifique a criação do LUN executando a seguinte API com a chave retornada:

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/luns/{key}

Exemplo de saída JSON

Você pode ver que o método POST de `/storage-provider/luns` invoca internamente todas as APIs necessárias para cada uma das funções e cria o objeto. Por exemplo, invoca o `/storage-provider/performance-service-levels/` API para atribuição do Nível de Serviço de Desempenho no LUN.

== Etapas de solução de problemas para falha na criação ou mapeamento de LUN

Ao concluir este fluxo de trabalho, você ainda poderá ver uma falha na criação do seu LUN. Mesmo que o LUN seja criado com sucesso, o mapeamento do LUN com o igroup pode falhar devido à indisponibilidade de um SAN LIF ou ponto de extremidade de acesso no nó no qual você cria o LUN. Em caso de falha, você poderá 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.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PUBLICAR	/storage-provider/access-endpoints

Exemplo de cURL

Você deve inserir os detalhes do ponto de extremidade de acesso que deseja criar, como 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 parceiro do nó inicial. Quando você executa esta operação, ela cria pontos de extremidade de acesso no nó inicial e no nó parceiro.

2. Consulte o trabalho com a chave do objeto Job retornada na saída JSON para verificar se ele foi executado com sucesso para adicionar os pontos de extremidade de acesso no SVM e se os serviços iSCSI/FCP foram habilitados no SVM.

Categoria	verbo HTTP	Caminho
servidor de gerenciamento	PEGAR	/management-server/jobs/{key}

Exemplo de saída JSON

No final da saída, você pode ver a chave dos pontos de extremidade de acesso criados. Na saída a seguir, o valor `"name": "accessEndpointKey"` indica o ponto de extremidade de acesso criado no nó inicial do LUN, para o qual a chave é `9c964258-14ef-11ea-95e2-00a098e32c28`. O valor `"name": "accessEndpointHAKKey"` indica o ponto de extremidade de acesso criado no nó parceiro do nó inicial, para o qual a chave é `9d347006-14ef-11ea-8760-00a098e3215f`.

3. Modifique o LUN para atualizar o mapeamento do igroup. Para obter mais informações sobre modificação de fluxo de trabalho, consulte “Modificando cargas de trabalho de armazenamento”.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	CORREÇÃO	/storage-provider/lun/{key}

Na entrada, especifique a chave `igroup` com a qual você deseja atualizar o mapeamento LUN, juntamente com a chave `LUN`.

Exemplo de cURL

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 do LUN consultando com a chave LUN.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/luns/{key}

Exemplo 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 provisionado inicialmente.

Modifique cargas de trabalho de armazenamento usando APIs

Modificar cargas de trabalho de armazenamento consiste em atualizar LUNs ou compartilhamentos de arquivos com parâmetros ausentes ou alterar os parâmetros existentes.

Este fluxo de trabalho usa o exemplo de atualização de Níveis de Serviço de Desempenho para LUNs e compartilhamentos de arquivos.



O fluxo de trabalho pressupõe que o LUN ou compartilhamento de arquivos foi provisionado com Níveis de Serviço de Desempenho.

Modificar compartilhamentos de arquivos

Ao modificar um compartilhamento de arquivo, você pode atualizar os seguintes parâmetros:

- Capacidade ou tamanho.
- Configuração online ou offline.
- Política de Eficiência de Armazenamento.
- Nível de serviço de desempenho.
- Configurações da lista de controle de acesso (ACL).
- Exportar configurações de política. Você também pode excluir parâmetros da 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 como adicionar 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 arquivo CIFS ou NFS do compartilhamento de arquivo que você deseja atualizar. Esta API consulta todos os compartilhamentos de arquivos no seu data center. Pule esta etapa se você já souber a chave de compartilhamento de arquivo.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/file-shares

2. Veja os detalhes do compartilhamento de arquivos executando a seguinte API com a chave de compartilhamento de arquivos que você obteve.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/file-shares/{key}

Veja os detalhes do compartilhamento de arquivos 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 foi atribuída a ele.

Categoria	verbo HTTP	Caminho
Níveis de serviço de desempenho	PEGAR	/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 para `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.

Categoria	verbo HTTP	Caminho
Provedor de armazenamento	CORREÇÃO	/storage-provider/file-shares/{key}

Na entrada, você deve especificar apenas o parâmetro que deseja atualizar, juntamente com a chave de compartilhamento de arquivo. Neste caso, é a chave do Nível de Serviço de Desempenho.

Exemplo de cURL

```
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 inicial e parceiro foram criados com sucesso.

5. Verifique se o Nível de Serviço de Desempenho foi adicionado ao compartilhamento de arquivos usando a chave do objeto Job exibida na sua saída.

Categoria	verbo HTTP	Caminho
Servidor de gerenciamento	PEGAR	/management-server/jobs/{key}

Se você consultar pelo ID do objeto Job, verá se o compartilhamento de arquivos foi atualizado com sucesso. Em caso de falha, solucione o problema e execute a API novamente. Após a criação bem-sucedida, consulte o compartilhamento de arquivos para ver o objeto modificado:

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/file-shares/{key}

Veja os detalhes do compartilhamento de arquivos 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"
    }
  }
}
```

Atualizar LUNs

Ao atualizar um LUN, você pode modificar os seguintes parâmetros:

- Capacidade ou tamanho
- Configuração online ou offline
- Política de Eficiência de Armazenamento
- Nível de serviço de desempenho
- Mapa LUN



Durante uma única execução de API, você pode atualizar apenas um parâmetro.

Este procedimento descreve como adicionar 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 você deseja atualizar. Esta API retorna detalhes de todos os LUNS no seu data center. Pule esta etapa se você já conhece a chave LUN.

Categoria	verbo HTTP	Caminho
Provedor de armazenamento	PEGAR	/storage-provider/luns

2. Veja os detalhes do LUN executando a seguinte API com a chave LUN que você obteve.

Categoria	verbo HTTP	Caminho
Provedor de armazenamento	PEGAR	/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.

Exemplo 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.

Categoria	verbo HTTP	Caminho
Níveis de serviço de desempenho	PEGAR	/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 para `true`. Na saída, obtenha a chave do Nível de Serviço de Desempenho que você deseja aplicar ao LUN.

4. Aplique o Nível de Serviço de Desempenho no LUN.

Categoria	verbo HTTP	Caminho
Provedor de armazenamento	CORREÇÃO	/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.

Exemplo de cURL

```
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.

Categoria	verbo HTTP	Caminho
Provedor de armazenamento	PEGAR	/storage-provider/luns/{key}

Veja os detalhes do LUN na saída. Você pode ver que o Nível de Serviço de Desempenho está atribuído a este LUN.

Exemplo 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"
    }
  }
}

```

Modificar um compartilhamento de arquivo NFS usando APIs para oferecer suporte a CIFS

Você pode modificar um compartilhamento de arquivos NFS para suportar o protocolo CIFS. Durante a criação do compartilhamento de arquivos, é possível especificar parâmetros da lista de controle de acesso (ACL) e regras de política de exportação para o mesmo compartilhamento de arquivos. No entanto, se você quiser habilitar o CIFS no mesmo volume em que criou um compartilhamento de arquivos NFS, poderá atualizar os parâmetros de ACL nesse compartilhamento de arquivos para oferecer suporte ao CIFS.

Antes de começar

1. Um compartilhamento de arquivo 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 precisa 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 do trabalho, consulte *Provisionamento de compartilhamentos de arquivos CIFS e NFS*.

Isso se aplica a um compartilhamento de arquivos NFS que você criou adicionando apenas regras de política de exportação e não parâmetros de ACL. Você modifica o compartilhamento de arquivos NFS para incluir os parâmetros ACL.

Passos

1. No compartilhamento de arquivos NFS, execute um PATCH operação com os detalhes da ACL para permitir acesso CIFS.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	CORREÇÃO	/storage-provider/file-shares

Exemplo de cURL

Com base nos privilégios de acesso atribuídos ao grupo de usuários, conforme exibido no exemplo 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"
    }
  }
}
```

Exemplo de saída JSON

A operação retorna o ID do trabalho que executa a atualização.

2. Verifique se os parâmetros foram adicionados corretamente consultando os detalhes do compartilhamento de arquivos para o mesmo compartilhamento de arquivos.

Categoria	verbo HTTP	Caminho
provedor de armazenamento	PEGAR	/storage-provider/file-shares/{key}

Exemplo 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,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
    }
  }
}
```

Você pode ver a ACL atribuída junto 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 autorais

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas 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 e licenças de terceiros usados neste produto.

["Aviso para o Active IQ Unified Manager 9.16"](#)

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAIENTES; 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 DOCUMENTOS, 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.