Documentação do Active IQ Unified Manager

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/active-iq-unified-manager-918/index.html on November 13, 2026. Always check docs.netapp.com for the latest.

Índice

Documentação do Active IQ Unified Manager . . . 1
Notas de versão do Active IQ Unified Manager . . . 2
Comece agora . . . 3
- Comece a usar o Active IQ Unified Manager no VMware vSphere . . . 3
  - Requisitos do sistema . . . 3
  - Instale o Active IQ Unified Manager . . . 3
- Comece a usar o Active IQ Unified Manager no Linux . . . 4
  - Requisitos do sistema . . . 4
  - Instale o Active IQ Unified Manager . . . 4
- Comece a usar o Active IQ Unified Manager no Windows . . . 5
  - Requisitos do sistema . . . 5
  - Instale o Active IQ Unified Manager . . . 6

Instale o Unified Manager em sistemas VMware vSphere . . . 7
- Saiba mais sobre o Active IQ Unified Manager . . . 7
  - Saiba mais sobre o Active IQ Unified Manager . . . 7
  - Saiba o que o servidor Active IQ Unified Manager faz . . . 7
  - Saiba mais sobre a sequência de instalação do Active IQ Unified Manager . . . 7
- Requisitos para instalar o Unified Manager . . . 8
  - Certifique-se de que o servidor atenda aos requisitos de instalação do Active IQ Unified Manager . . . 8
  - Saiba mais sobre infraestrutura virtual e requisitos de hardware para o Active IQ Unified Manager . . . 8
  - Saiba mais sobre o software VMware e os requisitos de instalação do Active IQ Unified Manager . . . 10
  - Utilize navegadores compatíveis no Active IQ Unified Manager . . . 10
  - Saiba mais sobre os requisitos de protocolo e porta para o Active IQ Unified Manager . . . 11
  - Preencha a planilha no Active IQ Unified Manager . . . 14
- Instalação, atualização e remoção do Unified Manager no VMware vSphere . . . 16
  - Saiba mais sobre o processo de implantação do Active IQ Unified Manager . . . 16
  - Fluxo de trabalho de implantação do appliance virtual do Unified Manager . . . 16
  - Fluxo de trabalho de atualização do appliance virtual do Unified Manager . . . 20
  - Reinicie a máquina virtual do Active IQ Unified Manager . . . 23
  - Remover Active IQ Unified Manager . . . 23

Instale o Unified Manager em sistemas Linux . . . 25
- Introdução ao Active IQ Unified Manager . . . 25
  - Saiba mais sobre o Active IQ Unified Manager . . . 25
  - Entenda o que o servidor Active IQ Unified Manager faz . . . 25
  - Veja a sequência de instalação do Active IQ Unified Manager . . . 25
- Requisitos para instalar o Unified Manager . . . 26
  - Compreenda os requisitos para instalar o Active IQ Unified Manager . . . 26
  - Compreenda a infraestrutura virtual e os requisitos de hardware para o Active IQ Unified Manager . . . 26
  - Saiba mais sobre os requisitos de software Linux e de instalação no Active IQ Unified Manager . . . 28
  - Use navegadores compatíveis com o Active IQ Unified Manager . . . 30
  - Saiba mais sobre os requisitos de protocolo e porta no Active IQ Unified Manager . . . 31
  - Preencha a planilha no Active IQ Unified Manager . . . 34
- Instalar, atualizar e remover o software Unified Manager . . . 35

Instale, atualize e remova o Active IQ Unified Manager . . . 35
Entenda a sequência de instalação do Active IQ Unified Manager no Red Hat Enterprise Linux . . . 35
Instale o software necessário . . . 36
Configure o SELinux para compartilhamentos NFS e CIFS no Active IQ Unified Manager . . . 39
Instale o Unified Manager em sistemas Linux . . . 42
Atualizar o Unified Manager no Red Hat Enterprise Linux . . . 48
Atualize produtos de terceiros após a instalação do Unified Manager . . . 54
Reinicie o Active IQ Unified Manager . . . 55
Remover Active IQ Unified Manager . . . 55
Remova o usuário umadmin personalizado e o grupo de manutenção do Active IQ Unified Manager . . . 56
Instale o Unified Manager em sistemas Windows . . . 57
Introdução ao Active IQ Unified Manager . . . 57
Saiba mais sobre o Active IQ Unified Manager . . . 57
Saiba o que o servidor Active IQ Unified Manager faz . . . 57
Saiba mais sobre a sequência de instalação do Active IQ Unified Manager . . . 57
Requisitos para instalar o Unified Manager . . . 58
Certifique-se de que o servidor atenda aos requisitos de instalação do Active IQ Unified Manager . . . 58
Compreenda a infraestrutura virtual e os requisitos de hardware para o Active IQ Unified Manager . . . 58
Compreenda os requisitos de software e instalação do Windows para o Active IQ Unified Manager . . . 60
Utilize navegadores compatíveis no Active IQ Unified Manager . . . 61
Compreenda os requisitos de protocolo e porta para o Active IQ Unified Manager . . . 62
Preencha a planilha no Active IQ Unified Manager . . . 65
Instalar, atualizar e remover o software Unified Manager . . . 66
Saiba mais sobre o processo de instalação do Active IQ Unified Manager no Windows . . . 66
Instalar o Unified Manager no Windows . . . 67
Altere a senha do JBoss no Windows no Active IQ Unified Manager . . . 70
Utilize o caminho de atualização compatível para as versões do Active IQ Unified Manager . . . 71
Atualize o Active IQ Unified Manager no Windows . . . 72
Atualize produtos de terceiros . . . 73
Desinstale produtos de terceiros no Active IQ Unified Manager . . . 74
Reinicie o Active IQ Unified Manager no Windows . . . 75
Desinstale o Active IQ Unified Manager . . . 75
Execute tarefas de configuração e administração . . . 77
Configurar o Active IQ Unified Manager . . . 77
Saiba mais sobre como configurar o Active IQ Unified Manager . . . 77
Saiba mais sobre a sequência de configuração no Active IQ Unified Manager . . . 77
Acesse a interface web no Active IQ Unified Manager . . . 77
Execute a configuração inicial da interface web do Active IQ Unified Manager . . . 78
Adicionar clusters ao Active IQ Unified Manager . . . 80
Configurar notificações . . . 82
Alterar a senha do usuário local no Active IQ Unified Manager . . . 91
Defina o tempo limite de inatividade da sessão no Active IQ Unified Manager . . . 91
Defina o tempo limite da sessão usando a CLI no Active IQ Unified Manager . . . 92
Alterar o nome do host do Unified Manager . . . 92
Ative e desative o gerenciamento de storage baseado em políticas no Active IQ Unified Manager . . . 97

Configurar o Active IQ Unified Manager backup . . . 98
Gerenciar configurações de recursos . . . 98
Saiba mais sobre as configurações de recursos no Active IQ Unified Manager . . . 98
Habilite o gerenciamento de storage baseado em políticas no Active IQ Unified Manager . . . 99
Saiba mais sobre o recurso API Gateway no Active IQ Unified Manager . . . 99
Especifique o tempo limite de inatividade no Active IQ Unified Manager . . . 100
Ative os eventos do portal Active IQ no Active IQ Unified Manager . . . 100
Ative e desative as configurações de segurança para conformidade no Active IQ Unified Manager . . . 101
Ativar e desativar o upload de scripts no Active IQ Unified Manager . . . 102
Adicione um banner de login no Active IQ Unified Manager . . . 102
Use o console de manutenção . . . 102
Saiba mais sobre o console de manutenção no Active IQ Unified Manager . . . 102
Saiba mais sobre o usuário de manutenção no Active IQ Unified Manager . . . 103
Funcionalidades de diagnóstico do usuário no Active IQ Unified Manager . . . 103
Acesse o console de manutenção no Active IQ Unified Manager . . . 103
Acesse o console de manutenção usando o console da VM do vSphere no Active IQ Unified Manager 104
Menus do console de manutenção . . . 104
Altere a senha do usuário de manutenção no Windows no Active IQ Unified Manager . . . 110
Altere a senha umadmin do Active IQ Unified Manager em sistemas Linux . . . 110
Altere as portas que o Active IQ Unified Manager utiliza para os protocolos HTTP e HTTPS . . . 111
Adicionar interfaces de rede ao Active IQ Unified Manager . . . 111
Regere o certificado de cliente no Active IQ Unified Manager . . . 112
Adicionar espaço de disco . . . 112
Gerencie o acesso do usuário . . . 116
Adicionar usuários . . . 116
Editar configurações de usuário no Active IQ Unified Manager . . . 117
Visualizar usuários no Active IQ Unified Manager . . . 118
Excluir usuários ou grupos no Active IQ Unified Manager . . . 118
Saiba mais sobre controle de acesso baseado em funções no Active IQ Unified Manager . . . 119
Saiba mais sobre os tipos de usuários no Active IQ Unified Manager . . . 119
Saiba mais sobre as funções de usuário no Active IQ Unified Manager . . . 120
Saiba mais sobre funções e capacidades de usuário no Active IQ Unified Manager . . . 121
Gerenciar configurações de autenticação SAML . . . 122
Ative a autenticação SAML no Active IQ Unified Manager . . . 122
Utilize um provedor de identidade no Active IQ Unified Manager . . . 123
Ative a autenticação SAML no Active IQ Unified Manager . . . 124
Altere o provedor de identidade de autenticação SAML no Active IQ Unified Manager . . . 125
Atualize as configurações de autenticação SAML após uma alteração no certificado de segurança do Active IQ Unified Manager . . . 126
Desative a autenticação SAML no Active IQ Unified Manager . . . 127
Desative a autenticação SAML no console de manutenção do Active IQ Unified Manager . . . 127
Utilize a página de autenticação SAML no Active IQ Unified Manager . . . 128
Gerenciar autenticação . . . 129
Editar servidores de autenticação no Active IQ Unified Manager . . . 129
Excluir servidores de autenticação no Active IQ Unified Manager . . . 129

Autentique com o Active Directory ou OpenLDAP no Active IQ Unified Manager . . . 130
Registro de auditoria . . . 130
Utilize a página de autenticação remota no Active IQ Unified Manager . . . 133
Gerenciar certificados de segurança . . . 136
Visualize o certificado de segurança HTTPS no Active IQ Unified Manager . . . 136
Faça o download de uma solicitação de assinatura de certificado HTTPS no Active IQ Unified Manager . . . 136
Instale um certificado HTTPS assinado por uma Autoridade Certificadora (CA) no Active IQ Unified Manager . . . 137
Saiba mais sobre certificados HTTPS gerados usando ferramentas externas no Active IQ Unified Manager Unified Manager . . . 138
Descrições de páginas para gerenciamento de certificados . . . 140
Monitorar e gerenciar o armazenamento . . . 143
Introdução ao Active IQ Unified Manager . . . 143
Saiba mais sobre o Active IQ Unified Manager . . . 143
Saiba mais sobre monitoramento de saúde no Active IQ Unified Manager . . . 143
Saiba mais sobre monitoramento de desempenho no Active IQ Unified Manager . . . 144
Use as APIs REST do Active IQ Unified Manager . . . 145
O que o servidor Unified Manager faz . . . 145
Entenda a interface de usuário . . . 146
Saiba mais sobre a interface de usuário do Active IQ Unified Manager . . . 146
Layouts de janela típicos no Active IQ Unified Manager . . . 146
Personalizando o layout da janela no Active IQ Unified Manager . . . 147
Use a Ajuda do Active IQ Unified Manager . . . 148
Adicione aos favoritos seus tópicos de Ajuda no Active IQ Unified Manager . . . 149
Pesquise objetos de armazenamento no Active IQ Unified Manager . . . 149
Exporte os dados de armazenamento como relatórios no Active IQ Unified Manager . . . 150
Filtre o conteúdo da página de inventário no Active IQ Unified Manager . . . 151
Visualize os eventos ativos a partir do ícone de notificação no Active IQ Unified Manager . . . 153
Monitore e gerencie clusters a partir do painel de controle . . . 153
Monitore e gerencie clusters a partir do painel de controle no Active IQ Unified Manager . . . 153
Saiba mais sobre a página do painel de controle do Active IQ Unified Manager . . . 154
Corrija ou gerencie problemas do ONTAP diretamente do Unified Manager . . . 157
Gerencie clusters . . . 164
Aprenda como funciona o processo de descoberta de clusters no Active IQ Unified Manager . . . 164
Veja a lista de clusters monitorados pelo Active IQ Unified Manager . . . 165
Adicionar clusters ao Active IQ Unified Manager . . . 166
Edite as configurações do cluster no Active IQ Unified Manager . . . 168
Remover clusters do Active IQ Unified Manager . . . 169
Redescubra clusters no Active IQ Unified Manager . . . 169
Monitorar a infraestrutura virtual VMware . . . 170
Entenda como o Active IQ Unified Manager monitora a infraestrutura virtual VMware . . . 170
Visualize e adicione servidores vCenter no Active IQ Unified Manager . . . 174
Remover um vCenter Server do Active IQ Unified Manager . . . 176
Entenda como o Active IQ Unified Manager monitora máquinas virtuais . . . 176

Visualize a infraestrutura virtual em um cenário de recuperação de desastres com o Active IQ Unified Manager . . . 178
Provisionar e gerenciar cargas de trabalho . . . 180
Provisione e gerencie cargas de trabalho no Active IQ Unified Manager . . . 180
Visão geral das cargas de trabalho . . . 181
Gerenciar os níveis de serviço de desempenho . . . 188
Gerenciar políticas de eficiência de storage . . . 195
Gerencie e monitore as configurações do MetroCluster . . . 197
Saiba mais sobre o comportamento do volume durante o switchover e o switchback no Active IQ Unified Manager . . . 197
Entenda a conectividade do cluster em uma configuração do MetroCluster sobre FC no Active IQ Unified Manager . . . 199
Saiba mais sobre o MetroCluster por espelhamento de dados FC no Active IQ Unified Manager . . . 200
Monitore as configurações do MetroCluster no Active IQ Unified Manager . . . 201
Monitore a replicação do MetroCluster no Active IQ Unified Manager . . . 204
Gerenciar cotas . . . 205
Saiba mais sobre os limites de cota no Active IQ Unified Manager . . . 205
Visualize as quotas de usuários e grupos de usuários no Active IQ Unified Manager . . . 205
Crie regras para gerar endereços de e-mail no Active IQ Unified Manager . . . 205
Crie um formato de notificação por e-mail para cotas de usuários e grupos de usuários no Active IQ Unified Manager . . . 206
Edite os endereços de e-mail de cotas de usuários e grupos no Active IQ Unified Manager . . . 206
Entenda melhor as cotas . . . 207
Descrição das caixas de diálogo de quotas . . . 208
Solução de problemas . . . 211
Adicione espaço de disco ao diretório do banco de dados do Unified Manager . . . 211
Altere o intervalo de coleta de estatísticas de desempenho no Active IQ Unified Manager . . . 215
Altere o período de tempo que o Active IQ Unified Manager retém os dados de eventos e desempenho . . . 216
Resolver um erro de autenticação desconhecido no Active IQ Unified Manager . . . 217
Resolver o erro "Usuário não encontrado" no Active IQ Unified Manager . . . 217
Resolva o problema causado pela adição do LDAP usando outro serviço de autenticação no Active IQ Unified Manager . . . 217
Resolva um problema de rotação de logs do NetApp Manageability SDK no Active IQ Unified Manager . . . 218
Gerenciar eventos e alertas . . . 219
Gerenciar eventos . . . 219
Saiba mais sobre os eventos da plataforma Active IQ no Active IQ Unified Manager . . . 219
O que são os eventos do Event Management System . . . 219
Entenda como o Active IQ Unified Manager lida com um evento recebido . . . 224
Veja os detalhes do evento no Active IQ Unified Manager . . . 225
Visualize eventos não atribuídos no Active IQ Unified Manager . . . 226
Reconheça e resolva eventos no Active IQ Unified Manager . . . 226
Atribua eventos a usuários específicos no Active IQ Unified Manager . . . 227
Desative eventos indesejados no Active IQ Unified Manager . . . 228

Corrija problemas usando a correção automática no Active IQ Unified Manager . . . 229
Ativar e desativar o relatório de eventos do Active IQ no Active IQ Unified Manager . . . 230
Carregue um novo arquivo de regras do Active IQ no Active IQ Unified Manager . . . 231
Como o Active IQ Unified Manager gera eventos da plataforma Active IQ . . . 232
Resolva eventos da plataforma Active IQ no Active IQ Unified Manager . . . 232
Configure as configurações de retenção de eventos no Active IQ Unified Manager . . . 233
O que é uma janela de manutenção do Unified Manager . . . 233
Gerencie eventos de recursos do sistema host no Active IQ Unified Manager . . . 236
Entenda melhor os eventos . . . 236
Lista de eventos e tipos de gravidade . . . 241
Descrição das janelas de eventos e caixas de diálogo . . . 295
Gerenciar alertas . . . 307
Saiba mais sobre alertas no Active IQ Unified Manager . . . 307
Informações contidas em um e-mail de alerta do Active IQ Unified Manager . . . 307
Adicionar alertas . . . 308
Adicione alertas para eventos de desempenho no Active IQ Unified Manager . . . 311
Teste alertas no Active IQ Unified Manager . . . 312
Desative os alertas para eventos Resolvidos e Obsoletos no Active IQ Unified Manager . . . 312
Exclua os volumes de destino de recuperação de desastres da geração de alertas no Active IQ Unified Manager . . . 313
Visualize os alertas no Active IQ Unified Manager . . . 314
Editar alertas no Active IQ Unified Manager . . . 314
Excluir alertas no Active IQ Unified Manager . . . 314
Descrição das janelas de alerta e caixas de diálogo . . . 315
Gerenciar scripts . . . 321
Gerencie scripts no Active IQ Unified Manager . . . 321
Como os scripts funcionam com alertas no Active IQ Unified Manager . . . 321
Adicionar scripts no Active IQ Unified Manager . . . 322
Excluir scripts no Active IQ Unified Manager . . . 323
Execução de script de teste no Active IQ Unified Manager . . . 323
Saiba mais sobre os comandos da CLI do Active IQ Unified Manager compatíveis . . . 324
Descrição das janelas de script e caixas de diálogo . . . 329
Monitorar e gerenciar o desempenho do cluster . . . 331
Introdução ao monitoramento de desempenho do Active IQ Unified Manager . . . 331
Saiba mais sobre monitoramento de desempenho no Active IQ Unified Manager . . . 331
Explore os recursos de monitoramento de desempenho do Active IQ Unified Manager . . . 331
Use as interfaces do Active IQ Unified Manager para gerenciar o desempenho do sistema de storage 332
Visualize a configuração do cluster e os dados de desempenho no Active IQ Unified Manager . . . 332
Compreenda os ciclos de coleta de continuidade de dados no Active IQ Unified Manager . . . 334
Saiba mais sobre os registros de data e hora nos dados e eventos coletados no Active IQ Unified Manager . . . 335
Navegando pelos fluxos de trabalho de desempenho na interface gráfica do Unified Manager . . . 335
Navegue pelos fluxos de trabalho de desempenho na interface gráfica do Active IQ Unified Manager . 335
Faça login na interface do usuário do Active IQ Unified Manager . . . 335
Interface gráfica e caminhos de navegação . . . 336

Pesquise objetos de armazenamento no Active IQ Unified Manager . . . 342
Filtre o conteúdo da página de inventário no Active IQ Unified Manager . . . 343
Monitore o desempenho do cluster no Dashboard . . . 345
Monitore o desempenho do cluster a partir do painel no Active IQ Unified Manager . . . 345
Analise os painéis de desempenho no Active IQ Unified Manager Dashboard . . . 345
Interpretar mensagens de banners de desempenho no Active IQ Unified Manager . . . 346
Altere o intervalo de coleta de estatísticas de desempenho no Active IQ Unified Manager . . . 346
Solucione problemas de cargas de trabalho usando o analisador de carga de trabalho . . . 347
Solucione problemas de cargas de trabalho com o analisador de cargas de trabalho no Active IQ Unified Manager . . . 347
Compreenda os dados do analisador de carga de trabalho no Active IQ Unified Manager . . . 348
Entenda quando usar o analisador de carga de trabalho no Active IQ Unified Manager . . . 349
Utilize o analisador de carga de trabalho no Active IQ Unified Manager . . . 350
Monitore o desempenho do cluster na Performance Cluster Landing page . . . 350
Monitore o desempenho do cluster na página inicial de desempenho do cluster no Active IQ Unified Manager . . . 350
Entenda a página inicial do Cluster de Desempenho no Active IQ Unified Manager . . . 350
Página inicial do cluster de desempenho . . . 351
Monitore o desempenho usando as páginas de Inventário de Desempenho . . . 356
Monitore o desempenho de objetos usando as páginas de Inventário de Desempenho no Active IQ Unified Manager . . . 356
Visualize as páginas de inventário de desempenho para todos os objetos de storage no Active IQ Unified Manager . . . 357
Conteúdo da página de inventário do Refine Performance . . . 362
Analise as recomendações do Active IQ Unified Manager para o armazenamento em camadas de dados na nuvem . . . 365
Monitore o desempenho usando as páginas do Explorador de Desempenho . . . 366
Monitore o desempenho usando as páginas do Performance Explorer no Active IQ Unified Manager . . . 366
Utilize objetos raiz para monitoramento de desempenho no Active IQ Unified Manager . . . 367
Filtre objetos correlacionados na grade do Active IQ Unified Manager . . . 367
Especifique um intervalo de tempo para objetos correlacionados . . . 367
Defina objetos correlacionados para gráficos de comparação no Active IQ Unified Manager . . . 369
Entenda os gráficos de contadores no Active IQ Unified Manager . . . 370
Entenda os tipos de gráficos de contadores de desempenho no Active IQ Unified Manager . . . 371
Selecione os gráficos de desempenho a serem exibidos no Active IQ Unified Manager . . . 373
Expanda o painel Gráficos de Contadores no Active IQ Unified Manager . . . 374
Altere o foco dos gráficos de contador para um período mais curto no Active IQ Unified Manager . . . 374
Veja os detalhes do evento na linha do tempo de eventos do Active IQ Unified Manager . . . 375
Visualização ampliada dos gráficos de contadores . . . 376
Visualize a latência por componente de cluster no Active IQ Unified Manager . . . 378
Visualize o tráfego de IOPS da SVM por protocolo no Active IQ Unified Manager . . . 379
Visualize os gráficos de latência de volume e de LUN para verificar a garantia de desempenho no Active IQ Unified Manager . . . 379
Visualize o desempenho de todos os clusters SAN Array no Active IQ Unified Manager . . . 380
Visualize as IOPS do nó com base nas cargas de trabalho locais no Active IQ Unified Manager . . . 381

Componentes das páginas de destino do objeto . . . 381
Gerencie o desempenho usando informações do grupo de políticas de QoS . . . 387
Gerencie o desempenho usando informações do grupo de políticas de QoS no Active IQ Unified Manager . . . 387
Controle a taxa de transferência da carga de trabalho com QoS de storage no Active IQ Unified Manager . . . 387
Visualize os grupos de políticas de QoS disponíveis em todos os clusters no Active IQ Unified Manager . . . 389
Visualize volumes ou LUNs dentro do mesmo grupo de política de QoS no Active IQ Unified Manager 389
Visualize as configurações do grupo de políticas de QoS para volumes ou LUNs no Active IQ Unified Manager . . . 390
Compare volumes ou LUNs dentro do mesmo grupo de políticas de QoS no Active IQ Unified Manager . . . 391
Visualize as políticas de QoS em gráficos de throughput com o Active IQ Unified Manager . . . 391
Visualize as configurações mínimas e máximas de QoS da carga de trabalho no Active IQ Unified Manager . . . 393
Gerencie o desempenho usando informações sobre capacidade de desempenho e IOPS disponíveis . . . 394
Gerencie a capacidade de desempenho e os IOPS disponíveis no Active IQ Unified Manager . . . 394
Entenda o contador de capacidade de desempenho usada no Active IQ Unified Manager . . . 395
Utilize o valor de capacidade de desempenho usado no Active IQ Unified Manager . . . 396
Entenda as IOPS disponíveis no Active IQ Unified Manager . . . 396
Visualize os valores de capacidade de desempenho de nós e agregados utilizados no Active IQ Unified Manager . . . 398
Visualize os valores de IOPS disponíveis para nós e agregados no Active IQ Unified Manager . . . 398
Visualize os gráficos do contador de capacidade de desempenho no Active IQ Unified Manager . . . 399
Configure os limites de capacidade de desempenho utilizados no Active IQ Unified Manager . . . 401
Utilize o contador de capacidade de desempenho utilizada no Active IQ Unified Manager . . . 401
Entenda e use a página Node Failover Planning . . . 402
Utilize a página de Planejamento de Failover de Nós no Active IQ Unified Manager . . . 402
Determine as ações corretivas na página Planejamento de Failover de Desempenho/Nó no Active IQ Unified Manager . . . 402
Analise os componentes da página de Planejamento de Failover de Desempenho/Nó no Active IQ Unified Manager . . . 402
Crie políticas de limite para o planejamento de failover de nós no Active IQ Unified Manager . . . 404
Utilize o gráfico de detalhamento da capacidade de desempenho utilizada para o planejamento de failover no Active IQ Unified Manager . . . 404
Coletar dados e monitorar o desempenho da carga de trabalho . . . 406
Colete dados e monitore o desempenho da carga de trabalho no Active IQ Unified Manager . . . 406
Monitore os tipos de carga de trabalho com o Active IQ Unified Manager . . . 407
Compreenda os valores de medição de desempenho da carga de trabalho no Active IQ Unified Manager . . . 408
Entenda como o Active IQ Unified Manager calcula a faixa de desempenho esperada . . . 410
Utilize a previsão de latência para análise de desempenho no Active IQ Unified Manager . . . 411
Use a latência da carga de trabalho para identificar problemas de desempenho no Active IQ Unified Manager . . . 412

Avalie como as operações de cluster podem afetar a latência no Active IQ Unified Manager . . . 413
Monitore o desempenho do MetroCluster com o Active IQ Unified Manager . . . 414
Compreenda os eventos e alertas de desempenho . . . 415
Compreenda os eventos e alertas de desempenho no Active IQ Unified Manager . . . 415
Identifique as fontes de eventos de desempenho no Active IQ Unified Manager . . . 415
Priorize eventos de desempenho por gravidade no Active IQ Unified Manager . . . 416
Monitore as alterações de configuração detectadas pelo Active IQ Unified Manager . . . 416
Compreenda as políticas de limite de desempenho definidas pelo sistema no Active IQ Unified Manager . . . 417
Analise eventos de desempenho e notificações no Active IQ Unified Manager . . . 420
Entenda como o Active IQ Unified Manager determina o impacto no desempenho de um evento . . . 422
Compreenda os componentes do cluster e a contenção no Active IQ Unified Manager . . . 422
Identifique funções de carga de trabalho em eventos de desempenho no Active IQ Unified Manager . . . 425
Gerenciar limites de desempenho . . . 426
Gerencie os limites de desempenho no Active IQ Unified Manager . . . 426
Utilize políticas de limite de desempenho definidas pelo usuário no Active IQ Unified Manager . . . 426
Responda às políticas de limite de desempenho violadas no Active IQ Unified Manager . . . 428
Entenda os contadores de desempenho monitorados por meio de limites no Active IQ Unified Manager . . . 428
Compreenda os objetos de política de limite combinado e os contadores no Active IQ Unified Manager . . . 430
Crie políticas de limite de desempenho definidas pelo usuário no Active IQ Unified Manager . . . 431
Atribua políticas de limite de desempenho a objetos de storage no Active IQ Unified Manager . . . 432
Visualize as políticas de limite de desempenho no Active IQ Unified Manager . . . 433
Edite as políticas de limite de desempenho definidas pelo usuário no Active IQ Unified Manager . . . 433
Remova as políticas de limite de desempenho dos objetos de armazenamento no Active IQ Unified Manager . . . 434
Entenda as alterações nas políticas de limite de desempenho no Active IQ Unified Manager . . . 435
Gerencie políticas de limite ao mover objetos no Active IQ Unified Manager . . . 435
Analisar eventos de desempenho . . . 436
Analise eventos de desempenho no Active IQ Unified Manager . . . 436
Exibir informações sobre eventos de desempenho no Active IQ Unified Manager . . . 436
Analisar eventos a partir de limites de desempenho definidos pelo usuário . . . 437
Analisar eventos a partir de limites de desempenho definidos pelo sistema . . . 438
Analisar eventos a partir de limites de desempenho dinâmicos . . . 444
Resolver eventos de desempenho . . . 452
Resolva eventos de desempenho no Active IQ Unified Manager . . . 452
Confirme se a latência está dentro da faixa esperada no Active IQ Unified Manager . . . 452
Avalie como as alterações de configuração afetam o desempenho da carga de trabalho no Active IQ Unified Manager . . . 452
Melhore o desempenho da carga de trabalho ajustando as configurações do lado do cliente no Active IQ Unified Manager . . . 453
Entenda como problemas de cliente ou de rede afetam o desempenho no Active IQ Unified Manager . . . 453
Analise os volumes de alta atividade em um grupo de políticas de QoS no Active IQ Unified Manager 454
Mova os LIFs para melhorar o desempenho no Active IQ Unified Manager . . . 454

Execute operações de eficiência de storage em horários menos movimentados . . . 455
Entenda como a adição de discos afeta a realocação de dados no Active IQ Unified Manager . . . 456
Melhore o desempenho da carga de trabalho ativando o Flash Cache em um nó no Active IQ Unified Manager . . . 456
Melhore o desempenho da carga de trabalho ativando o Flash Pool em um agregado de storage no Active IQ Unified Manager . . . 457
Verifique a integridade da configuração do MetroCluster no Active IQ Unified Manager . . . 457
Verifique as configurações do MetroCluster no Active IQ Unified Manager . . . 457
Mova as cargas de trabalho para um agregado diferente no Active IQ Unified Manager . . . 458
Mova as cargas de trabalho para um nó diferente no Active IQ Unified Manager . . . 459
Mova as cargas de trabalho para um agregado em um nó diferente no Active IQ Unified Manager . . . 461
Mova as cargas de trabalho para um nó em um par de HA diferente no Active IQ Unified Manager . . . 462
Mova as cargas de trabalho para outro nó em um par de HA no Active IQ Unified Manager . . . 464
Use as configurações de política de QoS para priorizar as cargas de trabalho dos nós no Active IQ Unified Manager . . . 466
Remova volumes e LUNs inativos no Active IQ Unified Manager . . . 466
Entenda como a adição de discos afeta o layout do agregado no Active IQ Unified Manager . . . 467
Configure uma conexão entre um servidor Unified Manager e um provedor de dados externo . . . 467
Configure uma conexão entre o Active IQ Unified Manager e um provedor de dados externo . . . 467
Envie os dados de desempenho do Active IQ Unified Manager para um servidor externo . . . 467
Configure o Graphite para receber dados de desempenho do Active IQ Unified Manager . . . 468
Configure uma conexão entre o Active IQ Unified Manager e um provedor de dados externo . . . 469
Monitorar e gerenciar a integridade do cluster . . . 472
Introdução ao monitoramento de integridade do Active IQ Unified Manager . . . 472
Saiba mais sobre o monitoramento de integridade do Active IQ Unified Manager . . . 472
Entenda os recursos de monitoramento de integridade do Active IQ Unified Manager . . . 473
Use as interfaces do Active IQ Unified Manager para gerenciar a integridade do sistema de storage . . . 474
Gerenciar e monitorar clusters e a integridade dos objetos do cluster . . . 475
Entenda o monitoramento de clusters . . . 475
Visualize a lista de clusters e detalhes no Active IQ Unified Manager . . . 476
Verifique a integridade dos clusters em uma configuração MetroCluster no Active IQ Unified Manager 477
Visualize o status de integridade e capacidade de todos os clusters SAN Array no Active IQ Unified Manager . . . 479
Visualize a lista de nós e detalhes no Active IQ Unified Manager . . . 480
Gere um relatório de inventário de hardware para renovação de contrato no Active IQ Unified Manager . . . 481
Visualize a lista e os detalhes das VMs de armazenamento no Active IQ Unified Manager . . . 481
Veja a lista de agregados e os detalhes no Active IQ Unified Manager . . . 482
Veja as informações de capacidade do FabricPool no Active IQ Unified Manager . . . 482
Visualize os detalhes do pool de storage no Active IQ Unified Manager . . . 484
Veja a lista de volumes e detalhes no Active IQ Unified Manager . . . 484
Veja detalhes sobre os compartilhamentos NFS no Active IQ Unified Manager . . . 485
Veja detalhes sobre compartilhamentos SMB/CIFS no Active IQ Unified Manager . . . 486
Veja a lista de cópias de Snapshot no Active IQ Unified Manager . . . 486
Excluir cópias Snapshot no Active IQ Unified Manager . . . 487

Calcule o espaço recuperável para cópias Snapshot no Active IQ Unified Manager . . . 488
Compreenda as janelas e caixas de diálogo de objetos de cluster no Active IQ Unified Manager . . . 488
Fluxos de trabalho e tarefas comuns de integridade do Unified Manager . . . 489
Compreenda os fluxos de trabalho e tarefas comuns de saúde do Active IQ Unified Manager . . . 489
Monitorar e solucionar problemas de disponibilidade de dados . . . 490
Resolver problemas de capacidade . . . 497
Gerenciar limites de integridade . . . 498
Gerenciar objetivos de segurança do cluster . . . 504
Gerencie operações de backup e restauração . . . 515
Gerenciar scripts . . . 532
Gerenciar e monitorar grupos . . . 535
Priorize eventos de objetos de storage usando anotações . . . 543
Envie um pacote de suporte pela interface web e pelo console de manutenção . . . 551
Tarefas e informações relacionadas a diversos fluxos de trabalho . . . 558
Proteger e restaurar dados . . . 617
Criar e solucionar problemas em relacionamentos de proteção . . . 617
Tipos de proteção do SnapMirror no Active IQ Unified Manager . . . 617
Configure relações de proteção no Unified Manager . . . 619
Execute um failover e failback de uma relação de proteção . . . 621
Resolver uma falha em uma tarefa de proteção . . . 625
Resolva problemas de latência no Active IQ Unified Manager . . . 629
Gerenciar e monitorar relações de proteção . . . 630
Saiba como gerenciar e monitorar relações de proteção no Active IQ Unified Manager . . . 630
Visualize o status da proteção de volume no Active IQ Unified Manager . . . 631
Visualize as relações de proteção de volume no Active IQ Unified Manager . . . 633
Monitorar os relacionamentos LUN do Consistency Group no Active IQ Unified Manager . . . 633
Crie uma relação do SnapVault a partir da visualização Saúde: Todos os Volumes em Active IQ Unified Manager . . . 634
Crie uma relação de proteção do SnapVault na página de detalhes de Volume/Saúde do Active IQ Unified Manager . . . 635
Crie uma relação do SnapMirror a partir da visualização Saúde: Todos os Volumes no Active IQ Unified Manager . . . 636
Crie uma relação do SnapMirror a partir da página de detalhes de integridade do volume no Active IQ Unified Manager . . . 638
Crie uma relação do SnapMirror com replicação flexível em relação à versão no Active IQ Unified Manager . . . 639
Crie relações do SnapMirror com replicação flexível em relação à versão e capacidade de opção de reversão no Active IQ Unified Manager . . . 640
Configure as configurações de eficiência do destino no Active IQ Unified Manager . . . 641
Crie agendas de SnapMirror e SnapVault no Active IQ Unified Manager . . . 642
Amplie a proteção usando relações em cascata ou ramificação no Active IQ Unified Manager . . . 642
Edite as relações de proteção na página "Relações de Volume" no Active IQ Unified Manager . . . 643
Edite as relações de proteção na página Detalhes de Volume/Saúde no Active IQ Unified Manager . . . 644
Crie uma política do SnapMirror para maximizar a eficiência de transferência no Active IQ Unified Manager . . . 644

Crie uma política do SnapVault para maximizar a eficiência de transferência no Active IQ Unified Manager . . . 645
Cancelar uma transferência na página Relações de Volume em Active IQ Unified Manager . . . 645
Cancelar uma transferência na página de detalhes de Volume/Saúde no Active IQ Unified Manager . . . 646
Suspenda uma relação de proteção na página Relações de Volume no Active IQ Unified Manager . . . 647
Suspenda uma relação de proteção na página de detalhes de Volume/Saúde no Active IQ Unified Manager . . . 648
Desfaça uma relação do SnapMirror na página Relacionamentos de Volume do Active IQ Unified Manager . . . 649
Remova uma relação de proteção da página Relações de Volume em Active IQ Unified Manager . . . 649
Retome as transferências agendadas em uma relação inativa na página "Relacionamentos de Volume" no Active IQ Unified Manager . . . 650
Retome transferências em uma relação do SnapMirror inativa a partir da página de detalhes de Volume/Saúde no Active IQ Unified Manager . . . 650
Inicialize ou atualize as relações de proteção na página Relações de Volume do Active IQ Unified Manager . . . 651
Inicialize ou atualize as relações de proteção na página de detalhes de Volume/Integridade no Active IQ Unified Manager . . . 652
Ressincronize as relações de proteção na página "Relações de Volume" no Active IQ Unified Manager . . . 653
Reverta as relações de proteção na página "Relações de Volume" no Active IQ Unified Manager . . . 654
Restaure os dados usando as páginas de detalhes de Volume e Volume/Integridade em Active IQ Unified Manager . . . 655
Saiba mais sobre os pools de recursos no Active IQ Unified Manager . . . 656
Crie pools de recursos no Active IQ Unified Manager . . . 657
Editar pools de recursos no Active IQ Unified Manager . . . 657
Visualize o inventário do pool de recursos no Active IQ Unified Manager . . . 657
Adicionar membros do pool de recursos no Active IQ Unified Manager . . . 658
Remover agregados de pools de recursos em Active IQ Unified Manager . . . 658
Excluir pools de recursos no Active IQ Unified Manager . . . 659
Monitore as relações de proteção de recuperação de desastres da Storage VM . . . 659
Gerencie as associações de máquinas virtuais de armazenamento no Active IQ Unified Manager . . . 661
Requisitos de SVM e de pool de recursos para suportar serviços de storage no Active IQ Unified Manager . . . 664
Saiba mais sobre os jobs no Active IQ Unified Manager . . . 664
Monitore tarefas no Active IQ Unified Manager . . . 665
Veja os detalhes do trabalho no Active IQ Unified Manager . . . 665
Cancelar tarefas no Active IQ Unified Manager . . . 665
Tente novamente uma tarefa de proteção com falha no Active IQ Unified Manager . . . 666
Descrição das janelas e caixas de diálogo de relacionamentos de proteção . . . 666
Gere relatórios personalizados . . . 708
Relatórios do Unified Manager . . . 708
Saiba mais sobre os relatórios do Active IQ Unified Manager . . . 708
Pontos de acesso para geração de relatórios . . . 708
Compreenda os relatórios no Active IQ Unified Manager . . . 710

Compreenda a relação entre visualização e relatório no Active IQ Unified Manager . . . 710
Saiba mais sobre os tipos de relatórios no Active IQ Unified Manager . . . 711
Compreenda as limitações de geração de relatórios no Active IQ Unified Manager . . . 712
Trabalhe com relatórios . . . 713
Compreenda os fluxos de trabalho de relatórios no Active IQ Unified Manager . . . 713
Comece a gerar relatórios no Active IQ Unified Manager . . . 714
Pesquise um relatório agendado no Active IQ Unified Manager . . . 717
Personalize relatórios . . . 717
Baixe relatórios no Active IQ Unified Manager . . . 721
Agendar relatórios . . . 721
Agende relatórios no Active IQ Unified Manager . . . 721
Agende um relatório . . . 721
Gerenciar cronogramas de relatórios . . . 724
Exemplos de relatórios personalizados . . . 726
Entenda os exemplos de relatórios personalizados no Active IQ Unified Manager . . . 726
Personalize os relatórios de armazenamento do cluster . . . 727
Personalize os relatórios de capacidade do agregado . . . 730
Personalize os relatórios de capacidade de volume . . . 732
Personalize os relatórios de capacidade do Qtree . . . 735
Personalize relatórios de compartilhamento NFS . . . 736
Personalize os relatórios de VMs de armazenamento . . . 737
Personalize os relatórios de relacionamento de volume . . . 739
Personalize os relatórios de desempenho de volume . . . 743
Exemplos de relatórios do Microsoft Excel . . . 744
Entenda exemplos de relatórios do Microsoft Excel no Active IQ Unified Manager . . . 744
Crie um relatório para exibir uma tabela e um gráfico de capacidade agregada no Active IQ Unified Manager . . . 744
Exibir gráficos de capacidade total agregada versus capacidade disponível no Active IQ Unified Manager . . . 747
Crie um relatório para visualizar gráficos de capacidade de volume disponível no Active IQ Unified Manager . . . 750
Crie um relatório para visualizar os agregados com o maior número de IOPS disponíveis no Active IQ Unified Manager . . . 753
Gerencie o armazenamento usando APIs REST . . . 756
Primeiros passos com Active IQ Unified Manager . . . 756
Comece a usar as APIs REST do Active IQ Unified Manager . . . 756
Identifique os usuários pretendidos das Active IQ Unified Manager REST APIs . . . 756
Gerencie o acesso à API e as categorias do Active IQ Unified Manager . . . 756
Entenda os serviços REST oferecidos no Active IQ Unified Manager . . . 758
Entenda os números de versão da API no Active IQ Unified Manager . . . 759
Entenda o modelo de recursos de armazenamento do ONTAP no Active IQ Unified Manager . . . 759
Acesso à API REST e autenticação no Active IQ Unified Manager . . . 760
Acesse e autentique APIs REST no Active IQ Unified Manager . . . 760
Saiba mais sobre os códigos de status HTTP do Active IQ Unified Manager . . . 763
Siga as práticas recomendadas para usar o Active IQ Unified Manager APIs . . . 764

Solucione problemas com registros do sistema no Active IQ Unified Manager . . . 764
Entenda como o Active IQ Unified Manager utiliza objetos Job para processamento assíncrono . . . 765
Saiba mais sobre o programa de exemplo do servidor Hello API no Active IQ Unified Manager . . . 766
APIs REST do Unified Manager . . . 770
Entenda as categorias para as APIs REST do Active IQ Unified Manager . . . 770
Gerencie objetos de armazenamento em um data center usando APIs no Active IQ Unified Manager . 771
Acesse as APIs do ONTAP por meio de acesso proxy no Active IQ Unified Manager . . . 777
Execute tarefas administrativas usando APIs no Active IQ Unified Manager . . . 780
Gerencie usuários no Active IQ Unified Manager usando APIs . . . 782
Visualize métricas de desempenho usando APIs no Active IQ Unified Manager . . . 783
Visualize tarefas e detalhes do sistema usando APIs no Active IQ Unified Manager . . . 793
Gerencie eventos e alertas usando APIs no Active IQ Unified Manager . . . 794
Gerencie cargas de trabalho . . . 797
Fluxos de trabalho comuns para gerenciamento de storage . . . 805
Compreenda os fluxos de trabalho comuns da API para gerenciamento de storage no Active IQ Unified Manager . . . 805
Identifique problemas de espaço em agregados usando as APIs do Active IQ Unified Manager . . . 806
Identifique problemas com objetos de armazenamento usando o Active IQ Unified Manager event APIs . . . 808
Solucione problemas dos volumes ONTAP usando as APIs de gateway do Active IQ Unified Manager 809
Fluxos de trabalho para gerenciamento de carga de trabalho . . . 812
Avisos legais . . . 837
Direitos autorais . . . 837
Marcas registradas . . . 837
Patentes . . . 837
Política de privacidade . . . 837
Código aberto . . . 837

Documentação do Active IQ Unified Manager

Notas de versão do Active IQ Unified Manager

Este documento apresenta um resumo das novas funcionalidades, limitações e problemas conhecidos do Active IQ Unified Manager 9.18.

Para obter mais informações, consulte o "Notas de versão do Active IQ Unified Manager".

Comece agora

Comece a usar o Active IQ Unified Manager no VMware vSphere

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

Requisitos do sistema

- Sistema operacional: VMware ESXi 8.0
- RAM: 12 GB
- CPU: 9572 MHz no total
- Espaço de disco livre: 5 GB (thin provisioning), 152 GB (thick provisioning)

Para obter requisitos de sistema detalhados, consulte o "Requisitos para instalar o Unified Manager" e "Matriz de Interoperabilidade".

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

Verificar integridade

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

Instale o Unified Manager

1. No vSphere Client, clique em **File > Deploy OVF Template**.
2. Localize o arquivo OVA e utilize o assistente para implantar o dispositivo virtual no servidor ESXi.
3. Na página Detalhes da Revisão, na seção Editor, a mensagem `Entrust Code Signing - OVCS2 (Trusted certificate)` confirma a integridade do arquivo baixado `OVA`. Para a mensagem `Entrust Code Signing - OVCS2 (Invalid certificate)`, atualize o VMware vCenter Server para a versão 7.0U3E ou superior.
4. Na página Customize Template, na guia Properties, preencha os campos conforme necessário para o tipo de instalação que você está realizando:
   - Para a configuração estática, insira as informações necessárias em todos os campos. Não é necessário adicionar informações ao 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 máquina virtual.
6. Clique na aba Console para visualizar o processo de inicialização inicial.
7. Configure o fuso horário.
8. Insira um nome de usuário e uma senha de manutenção do Unified Manager.

Ao final da instalação, são exibidas as informações para se conectar à interface da web do Unified Manager.

Comece a usar o Active IQ Unified Manager no Linux

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

Requisitos do sistema

- Sistema operacional: Red Hat Enterprise Linux versões 8.x e 9.4, com base na arquitetura x86_64, instalado usando o ambiente base "Server with GUI" da opção **Software Selection** do instalador do sistema operacional
- RAM: 12 GB, CPU: 9572 MHz no total
- Espaço livre em disco: 100 GB de espaço de disco no diretório `/opt/netapp/data`, 50 GB na partição raiz. Para os diretórios `/opt` e `/var/log` montados separadamente, certifique-se de que `/opt` tenha 15 GB, `/var/log` tenha 16 GB e `/tmp` tenha 10 GB de espaço livre.

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

Instale o Active IQ Unified Manager

Baixe o instalador

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

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

Verificar integridade

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

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

Verificar a configuração do repositório

Os procedimentos para configurar um repositório do Red Hat Enterprise Linux são específicos para cada ambiente. 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 as instruções para configurar o repositório do Red Hat Enterprise Linux.

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

Instale o Unified Manager

O Unified Manager utiliza o `yum` utilitário para instalar o software e qualquer software dependente. Como existem diferentes imagens do Red Hat Enterprise Linux, os pacotes instalados dependem do software presente nas imagens. O `yum` utilitário determina os pacotes de software dependentes para a instalação. Se você precisar de mais informações sobre os pacotes de software dependentes, consulte "Requisitos de software e instalação do Linux".

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

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

ou

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

Ao final da instalação, são exibidas as informações para se conectar à interface do usuário da web do Unified Manager. Caso você não consiga se conectar à interface da web, consulte o `README`arquivo incluído no pacote do software para obter mais informações sobre as restrições da porta 443.

Comece a usar o Active IQ Unified Manager no Windows

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

Requisitos do sistema

- Sistemas Operacionais
  - O Microsoft Windows Server 2019 Standard and Datacenter Edition
  - O Microsoft Windows Server 2022 Standard and Datacenter Edition

    O Unified Manager é compatível com sistema operacional Windows de 64 bits nos seguintes idiomas:

  - Inglês
  - Japonês
  - Chinês simplificado
- RAM: 12 GB
- CPU: 9572 MHz no total

- Espaço de disco livre: 100 GB de espaço de disco para o diretório de instalação e 50 GB de espaço de disco para o diretório de dados do MySQL

Para obter requisitos de sistema detalhados, consulte o "Requisitos para instalar o Unified Manager" e "Matriz de Interoperabilidade".

Instale o Active IQ Unified Manager

Baixe o instalador

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

Instale o Unified Manager

Para instalar o Unified Manager, certifique-se de que você tenha o Microsoft .NET 4.5.2 ou uma versão posterior instalada. Como parte do processo de instalação, o Unified Manager instala outros pacotes de terceiros, conforme necessário. Para obter mais informações sobre os pacotes de software dependentes, consulte o "Requisitos de software e instalação do Windows".

1. Faça login no Windows usando a conta de administrador local padrão.
2. No diretório em que 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 com o banco de dados, insira a senha de root do MySQL.
5. Siga as instruções restantes para concluir a instalação.
6. Clique em **Finish** ao final da instalação, e a interface da Web do Unified Manager é exibida.

Instale o Unified Manager em sistemas VMware vSphere

Saiba mais sobre o Active IQ Unified Manager

Saiba mais sobre o Active IQ Unified Manager

O Active IQ Unified Manager (formerly OnCommand Unified Manager) permite que você monitore e gerencie a integridade e o desempenho dos seus sistemas de storage 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 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

"NetApp Ferramenta de Matriz de Interoperabilidade"

Saiba o que o servidor Active IQ Unified Manager faz

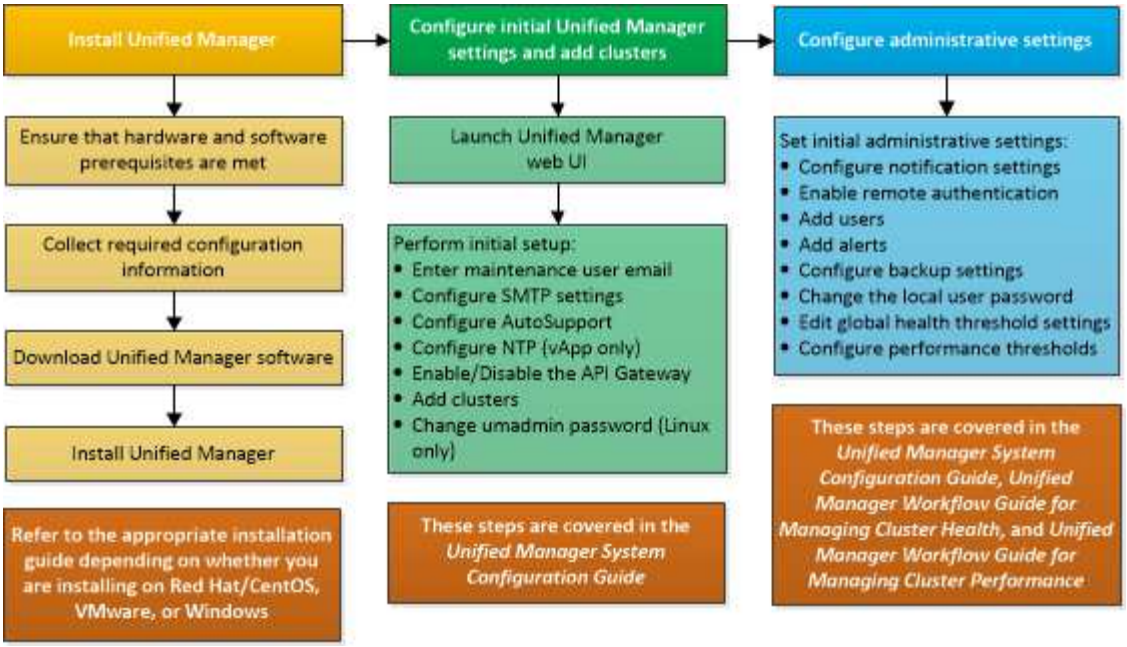
A infraestrutura do servidor do Unified Manager consiste em uma unidade de coleta de dados, um banco de dados e um servidor de aplicativos. Ela fornece serviços de infraestrutura como descoberta, monitoramento, controle de acesso baseado em funções (RBAC), auditoria e registro em log.

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

Saiba mais sobre a sequência de instalação do Active IQ Unified Manager

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

Certifique-se de que o servidor atenda aos requisitos de instalação do Active IQ Unified Manager

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

NetApp não oferece suporte a nenhuma modificação no código do aplicativo o Unified Manager. Se você precisar aplicar alguma medida de segurança ao servidor do Unified Manager, deverá fazer essas alterações no sistema operacional em que o Unified Manager está instalado.

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

"Suporte para medidas de segurança aplicadas ao Active IQ Unified Manager para o Clustered Data ONTAP"

Informações relacionadas

Para obter mais informações, consulte "NetApp Ferramenta de Matriz de Interoperabilidade"

Saiba mais sobre infraestrutura virtual e requisitos de hardware para o Active IQ Unified Manager

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

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

Configuração de hardware	Configurações recomendadas
RAM	12 GB
Processadores	4 CPUs
Capacidade de ciclos da CPU	9572 MHz no total (requisito mínimo de 9572 MHz)
Espaço livre em disco	• 5 GB (thin provisioning) • 152 GB (provisionamento thick)

O Unified Manager pode ser instalado em sistemas com pouca memória, mas os 12 GB de RAM recomendados garantem que haja memória suficiente para um desempenho ideal e para que o sistema possa acomodar clusters e objetos de storage adicionais à medida que sua configuração cresce. Você não deve definir limites de memória na máquina virtual em que o Unified Manager está implantado nem habilitar recursos (por exemplo, ballooning) que impeçam o software de utilizar a memória alocada no sistema.

Além disso, existe 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 limites de nós, recomendações de CPU e memória, consulte "o Guia de Práticas Recomendadas do Unified Manager".

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

Requisito para uso dedicado

O sistema físico ou virtual no qual você instala o Unified Manager deve ser usado exclusivamente para o Unified Manager e não deve ser compartilhado com outros aplicativos. 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 em um destino remoto. A melhor prática é identificar um local remoto externo ao sistema host do Unified Manager que tenha no mínimo 150 GB de espaço.

Requisitos para conectividade de host

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

Você pode usar o nome do host (ou o endereço IP do host) para acessar a interface web do produto. Se você configurou um endereço IP estático para sua rede durante a implantação, então designou um nome para o host da rede. Se você configurou a rede usando DHCP, deve 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 o endereço IP, sua configuração de rede precisa resolver esse nome curto para um FQDN válido.

Saiba mais sobre o software VMware e os requisitos de instalação do Active IQ Unified Manager

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 compatível é o VMware ESXi 8.0.

> Unified Manager OVA em sistemas VMware vSphere executa internamente o sistema operacional Debian OS 13 (Trixie). Para obter informações sobre as versões de hardware de máquina virtual que as versões suportadas dos servidores ESXi podem suportar, consulte a documentação da VMware.

As seguintes versões do vSphere são suportadas:

- O VMware vCenter Server 7.0 e 8.0

Consulte a Matriz de Interoperabilidade para obter a lista completa e mais atualizada das versões do ESXi compatíveis.

"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 uma falha de horário.

Requisitos de instalação

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

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

Se a implantação falhar em seu ambiente com High Availability ativada devido a recursos insuficientes, talvez seja necessário modificar as Cluster Features Virtual Machine Options desativando a VM Restart Priority e mantendo a Host Isolation Response ativada.

> Durante a instalação ou atualização do Unified Manager, o software de terceiros necessário e os patches de segurança 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 instalar ou atualizar de forma independente nenhum componente de terceiros.

Utilize navegadores compatíveis no Active IQ Unified Manager

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

A Interoperability Matrix contém a lista de versões de navegadores suportadas.

"mysupport.netapp.com/matrix"

Em todos os navegadores, desativar 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, também deve verificar a lista de navegadores compatíveis com o IdP.

Saiba mais sobre os requisitos de protocolo e porta para o Active IQ Unified Manager

As portas e os protocolos necessários permitem a comunicação entre o servidor do Unified Manager e os sistemas de armazenamento gerenciados, os 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 web do Unified Manager, pois as portas padrão são sempre utilizadas. Por exemplo, como o Unified Manager sempre tenta ser executado 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.
A interface do usuário da Web do Unified Manager e programas que usam APIs	HTTPS	443	Utilizado para acessar com segurança a interface do usuário da web do Unified Manager ou para fazer chamadas de API; as chamadas de API só podem ser feitas usando HTTPS.
Console de manutenção	SSH/SFTP	22	Utilizado 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
Syslog	UDP	514	Utilizado para acessar mensagens EMS baseadas em assinatura dos sistemas ONTAP e para criar eventos com base nessas mensagens.
REST	HTTPS	9443	Usado para acessar eventos EMS em tempo real baseados em API REST de sistemas ONTAP autenticados.
Banco de dados MySQL	O MySQL	3306	Utilizado para habilitar o acesso do OnCommand Workflow Automation e do OnCommand API Services ao Unified Manager.
Broker AMQP QPID	TCP/IP	56072	Usado para comunicação interna de mensagens.
Broker AMQP QPID	WebSocket sobre TCP	56080	Usada para escutar nesta porta mensagens recebidas do ONTAP (cloud agent).
Broker AMQP QPID	WebSocket sobre TCP	56443	Usada para escutar nesta porta as mensagens recebidas do ONTAP (agente na nuvem). A comunicação por esta porta suporta criptografia fornecida por TLS ou SSL.

A porta padrão do MySQL, 3306, fica restrita apenas ao localhost durante a instalação do Unified Manager em sistemas VMware vSphere. Isso não afeta nenhum cenário de upgrade, em que a configuração anterior é mantida. Essa configuração pode ser modificada, e a conexão pode ser disponibilizada para outros hosts usando a `Control access to MySQL port 3306` opção no console de manutenção. Para obter informações, consulte "Opções adicionais do 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 obter mais informações, consulte "Menus do console de manutenção".

Conexões do servidor do Unified Manager

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

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

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

Destino	Protocolo	Porta	Descrição
Sistema de storage	HTTPS	443/TCP	Utilizado 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 storage	NDMP	10000/TCP	Usado em determinadas operações de restauração de Snapshot.
AutoSupport servidor	HTTPS	443	Utilizado para enviar informações do AutoSupport. Requer 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	Utilizado para comunicação LDAP segura.	Servidor de e-mail
SMTP	25	Utilizado para enviar e-mails de notificação de alerta.	Remetente de trap SNMP

Destino	Protocolo	Porta	Descrição
SNMPv1 ou SNMPv3	162/UDP	Usado para enviar notificações de alerta por traps SNMP.	Servidor do provedor de dados externo
TCP	2003	Usado para enviar dados de desempenho a um provedor de dados externo, como o Graphite.	Servidor NTP
NTP	123/UDP	Utilizado para sincronizar a hora no servidor Unified Manager com um servidor de horário NTP externo. (apenas para sistemas VMware)	Broker AMQP QPID
TCP/IP	56072	Usado para comunicação interna de mensagens.	Broker AMQP QPID
WebSocket sobre TCP	56080	Usada para escutar nesta porta mensagens recebidas do ONTAP (cloud agent).	Broker AMQP QPID
WebSocket sobre TCP	56443	Usada para escutar nesta porta as mensagens recebidas do ONTAP (agente na nuvem). A comunicação por esta porta suporta criptografia fornecida por TLS ou SSL.	Syslog

Preencha a planilha no Active IQ Unified Manager

Antes de instalar e configurar o Unified Manager, você deve ter informações específicas sobre o seu ambiente prontamente disponíveis. Você pode registrar essas 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	
Nome de domínio totalmente qualificado do host	
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.

Configuração	Seu valor
Endereço de e-mail do usuário de manutenção	
Servidor NTP	
Nome do host do servidor SMTP ou endereço IP	
Nome de usuário SMTP	
Senha SMTP	
Porta SMTP	25 (Valor padrão)
E-mail a partir do qual as notificações de alerta são enviadas	
Nome do host ou endereço IP do servidor de autenticação	
Nome do administrador do Active Directory ou nome diferenciado de vinculação LDAP	
Senha do Active Directory ou senha de bind LDAP	
Nome diferenciado base do servidor de autenticação	
URL do provedor de identidade (IdP)	
Metadados do provedor de identidade (IdP)	
Endereços IP do host de destino de traps SNMP	
Porta SNMP	

Informações do cluster

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

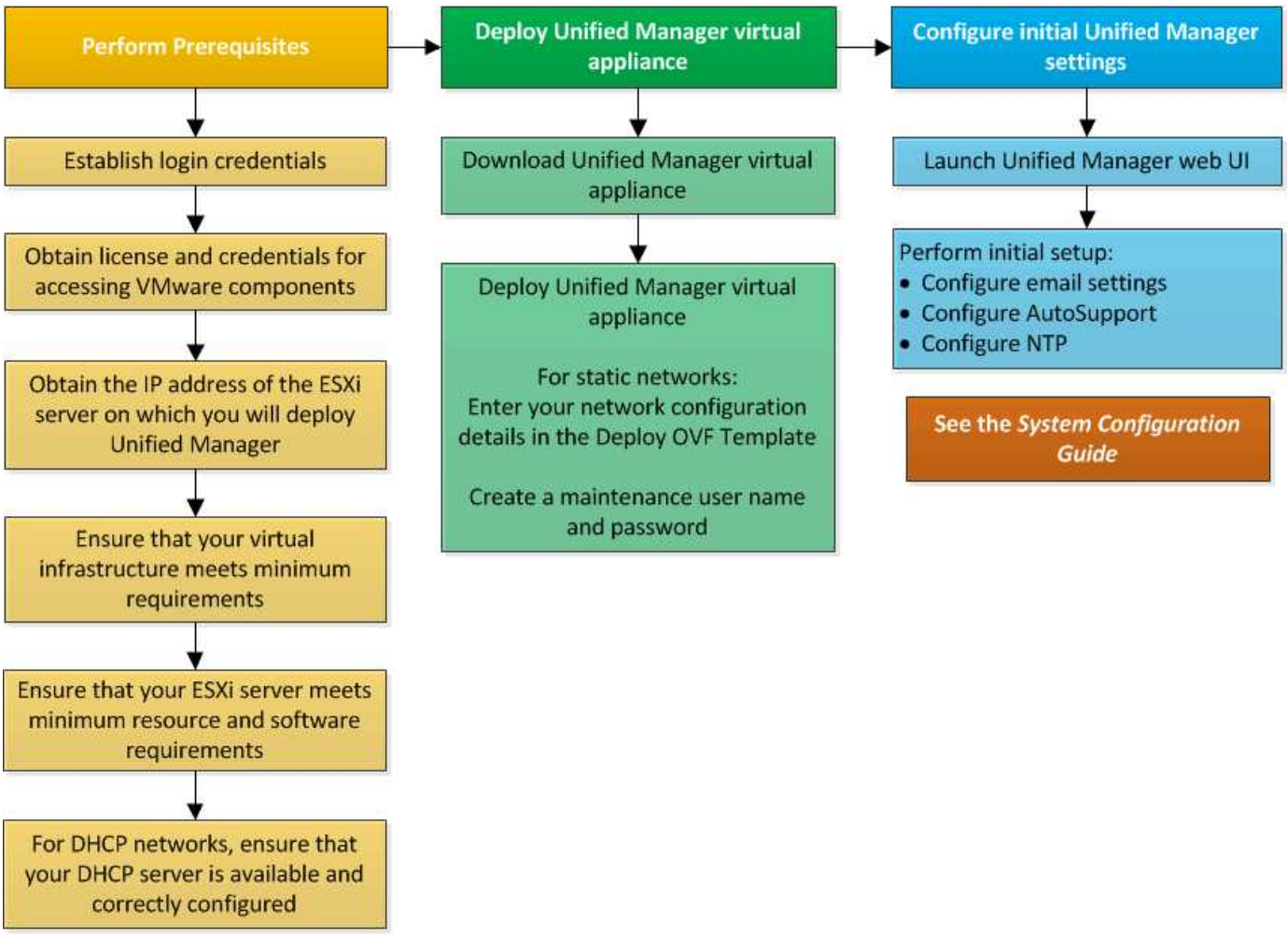
Cluster 1 de N	Seu valor
Nome do host ou endereço IP de gerenciamento do cluster	
Nome de usuário do administrador do ONTAP O administrador deve ter recebido a função “admin”.	

Cluster 1 de N	Seu valor
Senha do administrador do ONTAP	
Protocolo	HTTPS

Instalação, atualização e remoção do Unified Manager no VMware vSphere

Saiba mais sobre o processo de implantação do Active IQ Unified Manager

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



Fluxo de trabalho de implantação do appliance virtual do Unified Manager

Implantar o Active IQ 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 a implantação.

  Consulte "Requisitos do sistema".

- Certifique-se de que você tenha 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 storage no datastore e requisitos de memória
  - Você deve habilitar o IPv6 no host se planeja usar endereçamento IPv6.

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

Você deve acessar o console de manutenção usando o console da 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` ele já está incluído no pacote de instalação do Unified Manager.

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

Passos

1. Siga as etapas em "Baixe o Unified Manager".
2. Além disso, siga os passos em "Implante o dispositivo virtual do Unified Manager".

Baixe o arquivo de instalação do Active IQ Unified Manager

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

Antes de começar

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

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

Passos

1. Faça login no site de suporte da NetApp e acesse a página de download do Unified Manager:

   "NetApp site de suporte"

2. Selecione a versão necessária do Unified Manager e aceite o contrato de licença do usuário final.
3. Baixe e salve o `.tar` arquivo para a instalação do VMware vSphere em um diretório local ou de rede acessível ao seu vSphere Client.
4. Verifique o checksum 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 extrair o pacote do Unified Manager:

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

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

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

Implante o Active IQ Unified Manager appliance virtual

Após baixar o arquivo de instalação, você implanta o Unified Manager como um dispositivo virtual. Use o cliente Web do vSphere para implantar o dispositivo virtual em um servidor ESXi. Ao implantar o dispositivo virtual, você cria uma máquina virtual.

Antes de começar

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

Consulte "Requisitos de infraestrutura virtual".

Consulte "Requisitos de software e instalação do VMware".

Se você utiliza o Protocolo de Configuração Dinâmica de Hosts (DHCP), certifique-se de que o servidor DHCP esteja disponível e de que as configurações do DHCP e do adaptador de rede da máquina virtual (VM) estejam corretas. O DHCP é configurado por padrão.

Se você usa uma configuração de rede estática, certifique-se de que o endereço IP não esteja duplicado na mesma sub-rede e de 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 a disponibilidade de espaço de storage
- Se você não estiver usando DHCP, obtenha os endereços IPv4 ou IPv6 dos dispositivos de rede aos quais você pretende 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`* ele já 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 web do Unified Manager, você poderá ver um aviso do navegador sobre certificados não confiáveis.

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

Passos

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

   Na página de detalhes da avaliação:

   - Verifique os detalhes da seção Publisher. A mensagem **Entrust Code Signing - OVCS2 (Trusted certificate)** confirma a integridade do arquivo baixado `OVA`. + Se você vir a mensagem **Entrust Code Signing - OVCS2 (Invalid certificate)**, atualize o VMware vCenter Server para a versão 7.0U3E ou superior.

     Na página Customize Template:

   - Deixe todos os campos em branco ao usar DHCP e endereçamento IPv4.
   - Marque a caixa “Ativar endereçamento IPv6 automático” e deixe todos os outros campos em branco ao usar DHCP e endereçamento IPv6.
   - Se você quiser usar uma configuração de rede estática, poderá preencher os campos desta página, e essas configurações serão aplicadas durante a implantação. Certifique-se de que o endereço IP seja exclusivo do host no qual ele é implantado, que ainda não esteja em uso e que tenha uma entrada DNS válida.
3. Após a implantação do appliance virtual do Unified Manager no servidor ESXi, ligue a máquina virtual clicando com o botão direito do mouse nela e selecionando **Ligar**.

   Se a operação Power On falhar devido a recursos insuficientes, adicione recursos e tente a instalação 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 VM Console.

   Todas as informações de data exibidas utilizam o fuso horário configurado no Unified Manager, independentemente da configuração de fuso horário dos seus dispositivos gerenciados. Se seus sistemas de storage e o servidor de gerenciamento estiverem configurados com o mesmo servidor NTP, eles se referem ao mesmo instante no tempo, mesmo que apareçam de forma diferente. Por exemplo, se você criar uma cópia Snapshot usando um dispositivo configurado com um fuso horário diferente 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 isso…
DHCP	Selecione **Retry DHCP**. Se você pretende usar o DHCP, certifique-se de que ele esteja configurado corretamente. Se você usa uma rede com DHCP habilitado, as entradas de FQDN e do servidor DNS são fornecidas automaticamente ao dispositivo virtual. Se o DHCP não estiver configurado corretamente com DNS, o nome do host “UnifiedManager” será atribuído automaticamente e associado ao certificado de segurança. Se você não configurou uma rede com DHCP habilitado, deverá inserir manualmente as informações de configuração de rede.
Uma configuração de rede estática	a. Selecione **Insira os detalhes da configuração de rede estática**. O processo de configuração leva alguns minutos para terminar. b. Confirme os valores que você inseriu e selecione **Y**.

7. Quando solicitado, digite um nome de usuário para manutenção e clique em **Enter**.

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

8. Quando solicitado, digite uma senha e pressione **Enter**.

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

Você pode acessar a interface da Web para realizar a configuração inicial do Unified Manager, conforme descrito no "Configurando o Active IQ Unified Manager".

Fluxo de trabalho de atualização do appliance virtual do Unified Manager

Atualize o Active IQ Unified Manager

Você pode atualizar o Active IQ Unified Manager para a versão 9.18 somente a partir das versões 9.14 ou 9.16.

Durante o processo de atualização, o Unified Manager ficará indisponível. Você deve concluir todas as operações em andamento antes de atualizar o Unified Manager.

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

Se o seu sistema foi atualizado do Unified Manager 9.7, você não pode atualizar diretamente da

versão 9.14 para a 9.18 devido a alterações no sistema de arquivos nas versões do Debian. Em vez disso, siga este caminho de atualização: 9.14 → 9.16P2 → 9.18.

Passos

1. Siga as etapas em "Baixe a imagem ISO do Unified Manager".
2. Além disso, siga os passos descritos em "Atualizar o Unified Manager".

Utilize o caminho de atualização compatível para as versões do Active IQ 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 permitem uma atualização direta para versões posteriores. As atualizações do Unified Manager são limitadas ao modelo N-2. Isso significa que você só pode atualizar para as duas versões seguintes em todas as plataformas. Por exemplo, você só pode atualizar para o Unified Manager 9.18 a partir do Unified Manager 9.14 e do Unified Manager 9.16.

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

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

Exemplo de caminho de atualização:

1. Atualização 9.11 → 9.13
2. Atualização 9.13 → 9.14
3. Atualização 9.13 → 9.16
4. Atualização da versão 9.14 ou 9.16 para a versão 9.18

Para obter mais informações sobre a matriz de caminho de atualização, consulte isto "artigo da Knowledge Base (KB)".

Baixe o arquivo de atualização do Active IQ Unified Manager

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

Antes de começar

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

Passos

1. Faça login no site de suporte da NetApp:

   "NetApp site de suporte"

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

Atualize o appliance virtual do Active IQ Unified Manager

Você pode atualizar o appliance virtual do Active IQ Unified Manager das versões 9.14 ou 9.16 para a versão 9.18.

Antes de começar

Certifique-se do 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.

  Consulte "Requisitos de infraestrutura virtual".

  Consulte "Requisitos de software e instalação do VMware".

- Para usuários do vSphere 6.5 e versões posteriores, você instalou o VMware Remote Console (VMRC).
- Durante a atualização, talvez você seja 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. Ao confirmar, os dados históricos de desempenho são apagados após 6 meses.
- Você possui 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 do usuário de manutenção do Unified Manager

Durante o processo de atualização, o Unified Manager ficará indisponível. Você deve concluir todas as operações em andamento 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 **Home** > **Inventory** > **VMs and Templates**.
2. Selecione a máquina virtual (VM) na qual o appliance virtual do Unified Manager está instalado.
3. Se a máquina virtual 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 a aplicação.
5. No vSphere Client, ligue a máquina virtual 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. Faça login no console de manutenção do Unified Manager.
11. No menu principal, selecione **Atualizar**.

    Uma mensagem é exibida informando que o Unified Manager ficará indisponível durante o processo de

atualização e retomará após a conclusão.

12. Digite `y` para continuar.

    Uma mensagem de aviso é exibida, lembrando você de fazer backup da máquina virtual na qual o dispositivo virtual reside.

13. Digite `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 é desconectado automaticamente do console de manutenção.

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

Você pode abrir a interface da web em uma nova janela em um navegador compatível e fazer login para usar a versão atualizada do Unified Manager. Observe que é necessário aguardar a conclusão do processo de descoberta antes de executar qualquer tarefa na interface.

Reinicie a máquina virtual do Active IQ 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 appliance virtual deve estar ligado.
- Você deve estar conectado ao console de manutenção do Unified Manager como o usuário de manutenção.

Você também pode reiniciar a máquina virtual no vSphere usando a opção VMware **Restart Guest**. Consulte "o cmdlet Restart-VMGuest na referência de CMDLET do VMware vSphere PowerCLI da Broadcom."

Passos

1. No console de manutenção, selecione **System Configuration** > **Reboot Virtual Machine**.
2. Inicie a interface do usuário da web do Unified Manager no seu navegador e faça login.

Remover Active IQ 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 Workflow Automation deve ser encerrada.
- Todos os clusters (fontes de dados) devem ser removidos do servidor do Unified Manager antes de você remover a máquina virtual (VM).

Passos

1. Use o console de manutenção do Unified Manager para verificar se o servidor do Unified Manager não tem uma conexão ativa com um provedor de dados externo.
2. No vSphere Client, clique em **Home** > **Inventory** > **VMs and Templates**.
3. Selecione a máquina virtual que deseja remover e clique na guia **Resumo**.
4. Se a VM estiver em execução, clique em **Power** > **Shut Down Guest**.
5. Clique com o botão direito do mouse na VM que você deseja remover e clique em **Delete from Disk**.

Instale o Unified Manager em sistemas Linux

Introdução ao Active IQ Unified Manager

Saiba mais sobre o Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente OnCommand Unified Manager) permite que você monitore e gerencie a integridade e o desempenho de seus sistemas de storage 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 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

"NetApp Ferramenta de Matriz de Interoperabilidade"

Entenda o que o servidor Active IQ Unified Manager faz

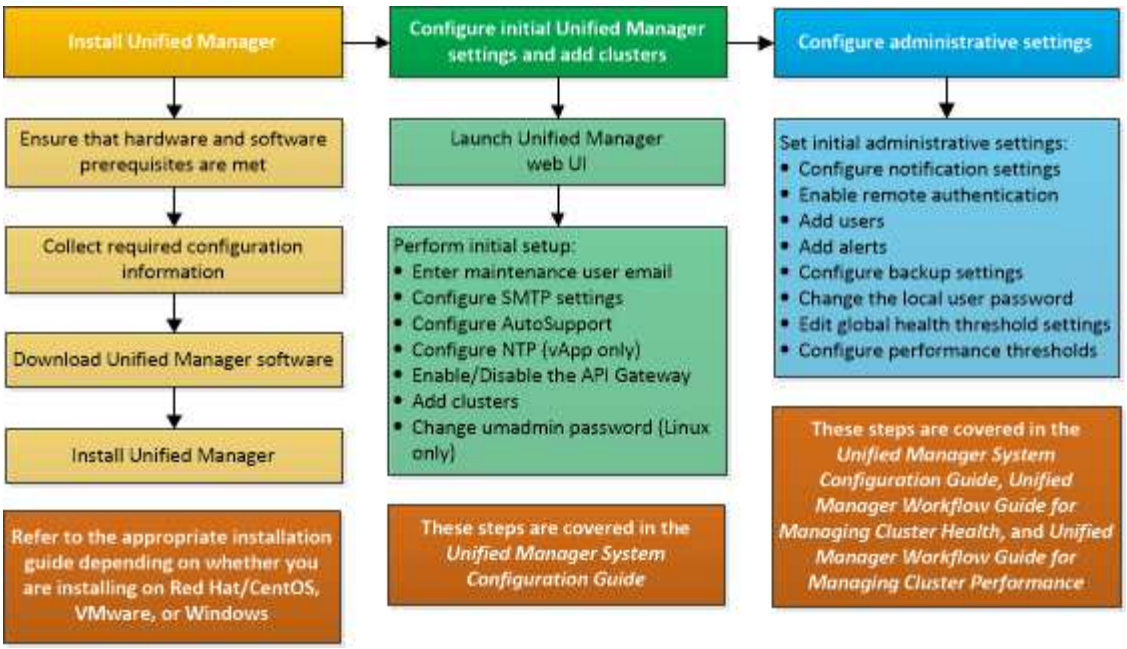
A infraestrutura do servidor do Unified Manager consiste em uma unidade de coleta de dados, um banco de dados e um servidor de aplicativos. Ela fornece serviços de infraestrutura como descoberta, monitoramento, controle de acesso baseado em funções (RBAC), auditoria e registro em log.

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

Veja a sequência de instalação do Active IQ Unified Manager

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

Compreenda os requisitos para instalar o Active IQ Unified Manager

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

NetApp não oferece suporte a nenhuma modificação no código do aplicativo o Unified Manager. Se você precisar aplicar alguma medida de segurança ao servidor do Unified Manager, deverá fazer essas alterações no sistema operacional em que o Unified Manager está instalado.

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

"Suporte para medidas de segurança aplicadas ao Active IQ Unified Manager para o Clustered Data ONTAP"

Informações relacionadas

"NetApp Ferramenta de Matriz de Interoperabilidade"

Compreenda a infraestrutura virtual e os requisitos de hardware para o Active IQ Unified Manager

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

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

Configuração de hardware	Configurações recomendadas
RAM	12 GB

Configuração de hardware	Configurações recomendadas
Processadores	4 CPUs
Capacidade de ciclos da CPU	9572 MHz no total (requisito mínimo de 9572 MHz)
Espaço livre em disco	150 GB, cuja capacidade é alocada da seguinte forma: • 50 GB alocados para a partição raiz • 100 GB de espaço livre em disco alocados ao `/opt/netapp/data` diretório, que está montado em uma unidade LVM ou em um disco local separado conectado ao sistema de destino Para diretórios montados separadamente `/opt` e `/var/log`, certifique-se de que `/opt` tenha 15 GB e `/var/log` tenha 16 GB de espaço livre. O diretório `/tmp` 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 para um desempenho ideal e para que o sistema possa acomodar clusters e objetos de storage adicionais à medida que sua configuração cresce. Você não deve definir limites de memória na máquina virtual em que o Unified Manager está implantado nem habilitar recursos (por exemplo, ballooning) que impeçam o software de utilizar a memória alocada no sistema.

Além disso, existe 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 limites de nós, recomendações de CPU e memória, consulte o "Guia de Práticas Recomendadas do Unified Manager".

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

Requisito para uso dedicado

O sistema físico ou virtual no qual você instala o Unified Manager deve ser usado exclusivamente para o Unified Manager e não deve ser compartilhado com outros aplicativos. 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 em um destino remoto. A melhor prática é identificar um local remoto externo ao sistema host do Unified Manager que tenha no mínimo 150 GB de espaço.

Requisitos para conectividade de host

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

Unified Manager seja concluída com êxito.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a interface web do produto. Se você configurou um endereço IP estático para sua rede durante a implantação, então designou um nome para o host da rede. Se você configurou a rede usando DHCP, deve 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 o endereço IP, sua configuração de rede precisa resolver esse nome curto para um FQDN válido.

Saiba mais sobre os requisitos de software Linux e de instalação no Active IQ Unified Manager

O sistema Linux no qual você instala o Unified Manager requer versões específicas do sistema operacional e do software de suporte. Para instalações em Linux, o Unified Manager pode ser instalado somente em um sistema operacional Red Hat Enterprise Linux. Ele não pode ser instalado em nenhum outro sistema operacional.

Software do sistema operacional

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

- As versões 8.x e 9.6 do Red Hat Enterprise Linux, baseadas na arquitetura x86_64

Consulte a Matriz de Interoperabilidade para obter a lista completa e mais atualizada das versões do Red Hat Enterprise Linux compatíveis.

"NetApp Matriz de interoperabilidade"

O servidor deve ser dedicado exclusivamente à execução do Unified Manager. Nenhum outro aplicativo deve ser instalado no servidor. Em alguns ambientes, um scanner de vulnerabilidades como o Qualys é instalado no sistema Linux devido à política da empresa. Você deve desativar o scanner de vulnerabilidades antes de instalar o Unified Manager para evitar falhas na instalação.

> Os scanners de vulnerabilidades, como o Qualys, podem levar ao alto uso da CPU ao analisar a máquina virtual (VM), seja internamente, quando o Unified Manager e o scanner de vulnerabilidades estão instalados na mesma VM, seja externamente, quando o Unified Manager e o scanner de vulnerabilidades estão instalados em dois servidores diferentes e o scanner de vulnerabilidades analisa a VM em que o Unified Manager está instalado. Esse problema geralmente faz com que a VM deixe de responder e afeta os serviços do Unified Manager. Portanto, a NetApp recomenda desativar o scanner de vulnerabilidades na VM em que o Unified Manager está instalado. Se desativar o scanner não for uma opção, analise a VM fora do horário comercial e reinicie os serviços após a conclusão da análise.

Software de terceiros

O Unified Manager é implantado em um servidor web WildFly. O WildFly 27.0.1.Final é fornecido e configurado juntamente 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 8.4.10 (do repositório MySQL)
- OpenJDK versão 17.0.14+6 (do repositório Red Hat Extra Enterprise Linux Server)
- Python 3.13.3 (do repositório Red Hat Extra Enterprise Linux Server)
- 7zip versão 7z2301-linux-x64. Para mais informações, consulte "Configure o pacote de software 7-zip".

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

Requisitos de autorização do usuário

O usuário raiz ou usuários sem privilégios de root podem instalar o Unified Manager em um sistema Linux usando o `sudo` comando.

Além disso, a instalação padrão do Unified Manager inclui o usuário umadmin (usuário padrão de manutenção) e o usuário jboss nos arquivos sudoers (`ocum_sudoers` e `ocie_sudoers`) no diretório `/etc/sudoers.d/`. Se você remover esse conteúdo do seu ambiente devido a políticas de segurança ou por causa de uma ferramenta de monitoramento de segurança, deverá adicioná-lo novamente. Você precisa preservar a configuração do sudoers, pois 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 em seu sistema estão listadas abaixo. Sistemas instalados ou configurados de maneira diferente, ou implantados fora do local (na nuvem), podem exigir etapas adicionais, e o Unified Manager pode não funcionar corretamente nessas implantações.

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

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

- Você precisa 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 em seu sistema, você deverá baixar e configurar o repositório manualmente.

  Consulte "Configurar manualmente o repositório EPEL".

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

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

Consulte "Configuração manual do repositório MySQL".

- Você deve instalar apenas uma versão do Java no host do Unified Manager; caso contrário, o sistema poderá não conseguir determinar qual versão usar. Consulte "Após atualizar o Java no host do Active IQ Unified Manager, os serviços não iniciam.".

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 externas de software do seu sistema. Em seguida, você poderá baixar o software necessário para o sistema conectado à internet e copiar os `.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 terceiro necessário de repositórios diferentes dos repositórios listados aqui. O software instalado a partir dos repositórios da Red Hat foi projetado especificamente para o Red Hat Enterprise Linux e está em conformidade com as melhores práticas da Red Hat (estruturas de diretórios, permissões etc.). O software de outros locais pode não seguir essas diretrizes, o que pode fazer a instalação do Unified Manager falhar ou causar problemas em 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, você pode não conseguir se conectar à interface do usuário da web do administrador após instalar o Unified Manager. Executar o seguinte comando permite o acesso à porta 443 para todos os usuários e aplicativos externos em uma instalação genérica do Red Hat Enterprise Linux.

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

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

```
# sudo yum install firewalld
```

Antes de executar os comandos, entre em contato com o departamento de TI para verificar se as políticas de segurança exigem um procedimento diferente.

O THP (Transparent Huge Pages) deve ser desativado em sistemas Red Hat. Quando ativado, em alguns casos, ele pode fazer com que o Unified Manager seja encerrado quando certos processos consomem memória demais e são finalizados.

Use navegadores compatíveis com o Active IQ Unified Manager

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

A Interoperability Matrix contém a lista de versões de navegadores suportadas.

"mysupport.netapp.com/matrix"

Em todos os navegadores, desativar 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, também deve verificar a lista de navegadores compatíveis com o IdP.

Saiba mais sobre os requisitos de protocolo e porta no Active IQ Unified Manager

As portas e os protocolos necessários permitem a comunicação entre o servidor do Unified Manager e os sistemas de armazenamento gerenciados, os 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 web do Unified Manager, pois as portas padrão são sempre utilizadas. Por exemplo, como o Unified Manager sempre tenta ser executado 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.
A interface do usuário da Web do Unified Manager e programas que usam APIs	HTTPS	443	Utilizado para acessar com segurança a interface do usuário da web do Unified Manager ou para fazer chamadas de API; as chamadas de API só podem ser feitas usando HTTPS.
Console de manutenção	SSH/SFTP	22	Utilizado 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	O MySQL	3306	Utilizado para habilitar o acesso do OnCommand Workflow Automation e do OnCommand API Services ao Unified Manager.
Syslog	UDP	514	Utilizado para acessar mensagens EMS baseadas em assinatura dos sistemas ONTAP e para criar eventos com base nessas mensagens.
REST	HTTPS	9443	Usado para acessar eventos EMS em tempo real baseados em API REST de sistemas ONTAP autenticados.
Banco de dados MySQL	O MySQL	3306	Utilizado para habilitar o acesso do OnCommand Workflow Automation e do OnCommand API Services ao Unified Manager.
Broker AMQP QPID	TCP/IP	56072	Usado para comunicação interna de mensagens.
Broker AMQP QPID	WebSocket sobre TCP	56080	Usada para escutar nesta porta mensagens recebidas do ONTAP (cloud agent).
Broker AMQP QPID	WebSocket sobre TCP	56443	Usada para escutar nesta porta as mensagens recebidas do ONTAP (agente na nuvem). A comunicação por esta porta suporta criptografia fornecida por TLS ou SSL.

A porta padrão do MySQL, 3306, fica restrita apenas ao localhost durante a instalação do Unified Manager em sistemas Linux. Isso não afeta nenhum cenário de upgrade, no qual a configuração anterior é mantida. Essa configuração pode ser modificada, e a conexão pode ser disponibilizada para outros hosts usando a `Control access to MySQL port 3306` opção no console de manutenção. Para obter informações, consulte "Opções adicionais do 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 obter mais informações, consulte "Menus do console de manutenção".

Conexões do servidor do Unified Manager

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

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

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

Destino	Protocolo	Porta	Descrição
Sistema de storage	HTTPS	443/TCP	Utilizado para monitorar e gerenciar sistemas de armazenamento.
Sistema de storage	NDMP	10000/TCP	Usado em determinadas operações de restauração de Snapshot.
AutoSupport servidor	HTTPS	443	Utilizado para enviar informações do AutoSupport. Requer 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	Utilizado para comunicação LDAP segura.	Servidor de e-mail
SMTP	25	Utilizado para enviar e-mails de notificação de alerta.	Remetente de trap SNMP
SNMPv1 ou SNMPv3	162/UDP	Usado para enviar notificações de alerta por traps SNMP.	Servidor do provedor de dados externo
TCP	2003	Usado para enviar dados de desempenho a um provedor de dados externo, como o Graphite.	Servidor NTP
NTP	123/UDP	Utilizado para sincronizar a hora no servidor Unified Manager com um servidor de horário NTP externo. (apenas para sistemas VMware)	Syslog

Destino	Protocolo	Porta	Descrição
UDP	514	Utilizado pelo Unified Manager para enviar registros de auditoria para um servidor syslog remoto.	Broker AMQP QPID
TCP/IP	56072	Usado para comunicação interna de mensagens.	Broker AMQP QPID
WebSocket sobre TCP	56080	Usada para escutar nesta porta mensagens recebidas do ONTAP (cloud agent).	Broker AMQP QPID

Preencha a planilha no Active IQ Unified Manager

Antes de instalar e configurar o Unified Manager, você deve ter informações específicas sobre o seu ambiente prontamente disponíveis. Você pode registrar essas 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
Nome de domínio totalmente qualificado do host	
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.

Configuração	Seu valor
Endereço de e-mail do usuário de manutenção	
Nome do host do servidor SMTP ou endereço IP	
Nome de usuário SMTP	
Senha SMTP	

Configuração	Seu valor
Porta SMTP	25 (Valor padrão)
E-mail a partir do qual as notificações de alerta são enviadas	
Nome do host ou endereço IP do servidor de autenticação	
Nome do administrador do Active Directory ou nome diferenciado de vinculação LDAP	
Senha do Active Directory ou senha de bind LDAP	
Nome diferenciado base do servidor de autenticação	
URL do provedor de identidade (IdP)	
Metadados do provedor de identidade (IdP)	
Endereços IP do host de destino de traps 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 do cluster	
Nome de usuário do administrador do ONTAP O administrador deve ter recebido a função “admin”.	
Senha do administrador do ONTAP	
Protocolo	HTTPS

Instalar, atualizar e remover o software Unified Manager

Instale, atualize e remova o Active IQ Unified Manager

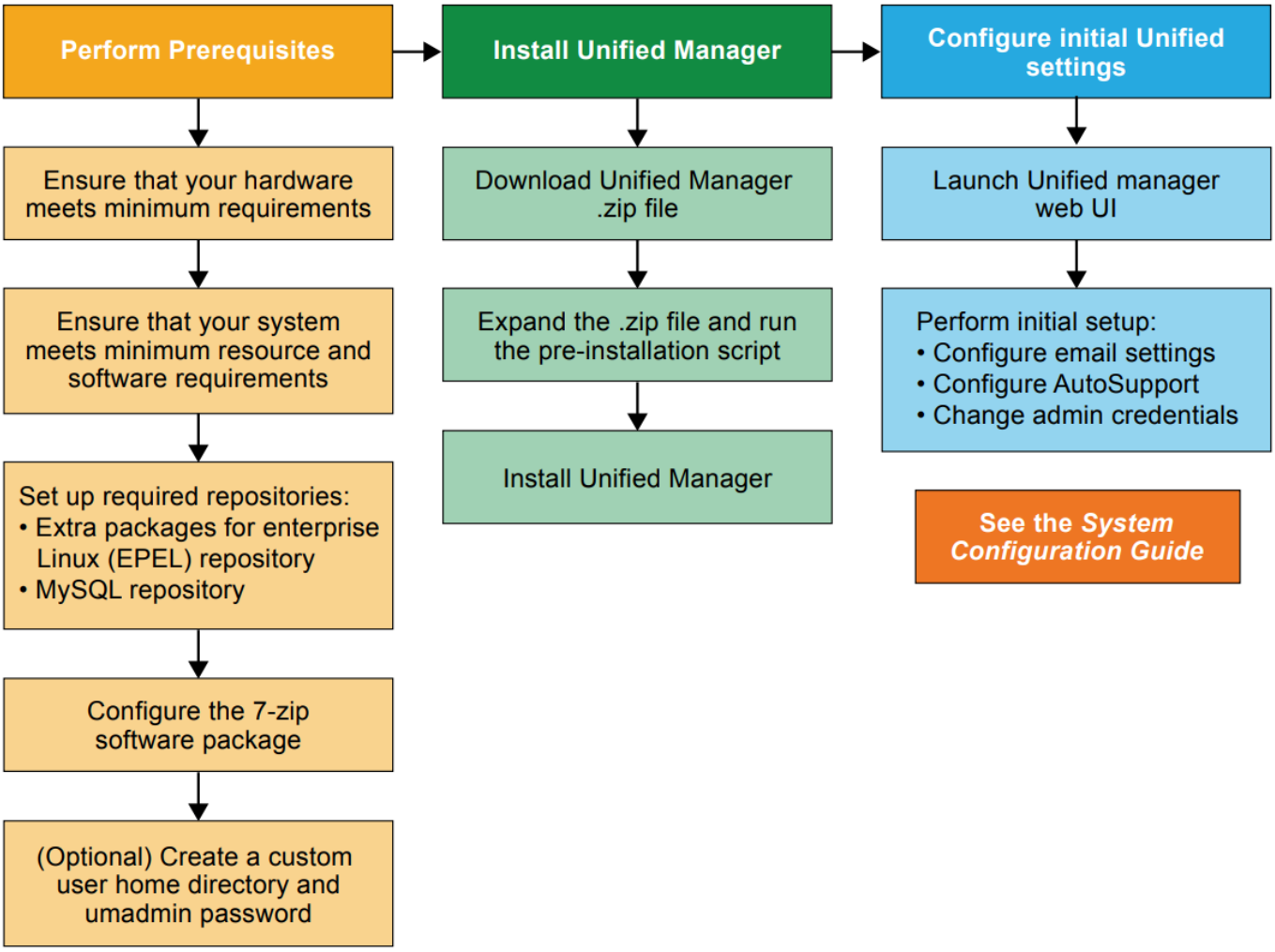
Em sistemas Linux, você pode instalar o software Unified Manager, atualizar para uma versão mais recente do software ou remover o Unified Manager.

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

Entenda a sequência de instalação do Active IQ Unified Manager no Red Hat Enterprise Linux

O fluxo de trabalho de instalação descreve as tarefas que você deve executar antes de

poder usar o Unified Manager.



Instale o software necessário

Configure o repositório EPEL para o Active IQ Unified Manager

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 terceiro necessários que devem ser instalados no seu sistema. Você usa o repositório EPEL para instalar o Unified Manager em um sistema Red Hat Enterprise Linux.

Passos

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

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

   Para a versão 9, faça o download em:

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

2. Configure o repositório EPEL:

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

Para sistemas do 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.

Configure o repositório MySQL para o Active IQ Unified Manager

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 que a instalação seja bem-sucedida.

O repositório do 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-o 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, faça o download 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
```

Em um sistema Red Hat Enterprise Linux 8, se você tiver repositórios internos com java-17-openjdk, 7-zip e outros pacotes de software fornecidos pelo repositório AppStream, você deve desativar o repositório AppStream e instalar o MySQL Community Server. Execute o seguinte comando:

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

Se você receber um erro de chave ausente ou de incompatibilidade de chave e a instalação falhar, tente estas etapas:

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

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

for example:

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

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

Configure o pacote de software 7-Zip no Active IQ Unified Manager

Para instalar com sucesso o Unified Manager em um sistema Red Hat Enterprise Linux, seu sistema deve estar configurado com acesso ao pacote de software 7-zip. Se o acesso à rede estiver disponível e a URL do 7-zip não estiver bloqueada por um firewall, o 7-zip será baixado automaticamente para o seu sistema durante um processo de instalação ou upgrade. NetApp recomenda o método de download automático.

Certifique-se de que a seguinte URL esteja desbloqueada no seu firewall para permitir que o Unified Manager baixe automaticamente o pacote de software 7-zip:
`https://7-zip.org/a/7z2301-linux-x64.tar.xz`

Alternativamente, você pode pré-instalar o 7-zip.

Pré-instale o pacote 7-zip

Você pode pré-instalar o 7-zip baixando-o manualmente ou usando um script incluído. Escolha um dos dois métodos a seguir:

Baixar usando um script incluído

Etapa

1. Execute o `install7zip.sh` script que está incluído no arquivo zip do Unified Manager.

Baixar manualmente

Certifique-se de baixar o pacote 7-zip somente do site oficial.

Passos

1. Baixe o pacote 7-zip (versão 23.01) do site oficial:

   `https://7-zip.org/a/7z2301-linux-x64.tar.xz`

2. Copie o arquivo para sua máquina virtual RHEL:

   ```
   7z2301-linux-x64.tar.xz
   ```

3. Extraia o arquivo:

```
sudo tar -xf 7z2301-linux-x64.tar.xz
```

4. Mova o `7zz` arquivo para o `/usr/bin/` diretório:

```
sudo cp 7zz /usr/bin/
```

5. Defina permissões de execução:

```
sudo chmod 755 /usr/bin/7zz
```

Verifique a instalação

Verifique se o pacote 7-zip foi instalado corretamente em seu sistema:

```
7zz -version
```

Configure o SELinux para compartilhamentos NFS e CIFS no Active IQ Unified Manager

Se você pretende montar `/opt/netapp` ou `/opt/netapp/data` em um dispositivo NAS ou SAN, e o SELinux estiver ativado, precisa estar ciente de algumas considerações.

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

Configure o contexto do SELinux quando `/opt/netapp/data` estiver montado

Se você tiver montado `/opt/netapp/data` no seu sistema e o SELinux estiver definido como `Enforcing`, certifique-se de que o tipo de contexto do SELinux para `/opt/netapp/data` esteja definido como `mysqld_db_t`, que é o elemento de contexto padrão para o local dos arquivos do 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 alterar esse contexto para `mysqld_db_t`.

2. Execute estas etapas para definir o contexto com base em como você montou `/opt/netapp/data`.
   a. Execute os seguintes comandos para definir o contexto 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 a `/opt/netapp/data/` opção de montagem, adicione o rótulo MySQL da seguinte forma:

      `context=system_u:object_r:mysqld_db_t:s0`

   c. Desmonte e remonte `/opt/netapp/data/` para habilitar o contexto.
   d. Se você tiver uma montagem NFS direta, execute o seguinte comando para definir o contexto como `mysqld_db_t`:

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

3. Verifique se o contexto está configurado 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/
```

Configure o contexto do SELinux quando `/opt/netapp` estiver montado e `/opt/netapp/data/` também estiver montado separadamente

Neste cenário, em primeiro lugar, você deve definir o contexto para `/opt/netapp/data/` conforme descrito na seção anterior. Após definir o contexto correto para `/opt/netapp/data/`, certifique-se de que o diretório pai `/opt/netapp` não tenha 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
   ```

   Neste resultado, o contexto `file_t`deve ser alterado. Os comandos a seguir definem o contexto como `usr_t`. Você pode definir o contexto como 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 o 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` o MySQL em `/etc/fstab`, edite o arquivo `/etc/fstab`. Para a opção de montagem `/opt/netapp`, adicione o rótulo do MySQL da seguinte forma:

   `context=system_u:object_r:usr_t:s0`

2. Desmonte e depois 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 configurado corretamente:

      `ls -dZ /opt/netapp`

   Uma saída de exemplo

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

Configure o contexto do SELinux quando `/opt/netapp` estiver montado e `/opt/netapp/data/` não estiver montado separadamente

Se você tiver montado `/opt/netapp` no seu sistema e o SELinux estiver definido como `Enforcing`, certifique-se de que o tipo de contexto do SELinux para `/opt/netapp` esteja definido como `mysqld_db_t`, que é o elemento de contexto padrão para o local dos arquivos do 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 alterar esse contexto para `mysqld_db_t`.

2. Execute os seguintes passos para definir o contexto com base em como você o montou `/opt/netapp`.
   a. 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
```

b. Se você configurou `/opt/netapp`o MySQL em `/etc/fstab`<caminho_para_o_arquivo>`, edite o `/etc/fstab`arquivo. Para a `/opt/netapp/`opção de montagem, adicione o rótulo MySQL da seguinte forma:
`context=system_u:object_r:mysqld_db_t:s0

c. Desmonte e, em seguida, monte novamente `/opt/netapp/` para habilitar o contexto.

d. Se você tiver uma montagem NFS direta, execute o seguinte comando para definir o contexto como `mysqld_db_t`:
`mount <nfsshare>:/<mountpoint> /opt/netapp -o context=system_u:object_r:mysqld_db_t:s0`

3. Verifique se o contexto está configurado corretamente:

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

Um exemplo de saída:

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

Instale o Unified Manager em sistemas Linux

Crie um diretório base de usuário personalizado e uma senha umadmin antes de instalar o Active IQ Unified Manager

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

Antes de começar

- O sistema deve atender aos requisitos descritos em "Requisitos de hardware do sistema".
- Você deve conseguir fazer login como o usuário raiz no sistema Red Hat Enterprise Linux.

A instalação padrão do Unified Manager executa as seguintes tarefas:

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

Como alguns ambientes de instalação restringem o acesso a `/home`, a instalação falha. Você deve criar o diretório base em um local diferente. Além disso, alguns sites podem ter regras sobre a complexidade da senha 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 da instalação, siga estas etapas para criar um diretório base personalizado e definir a senha do usuário umadmin.

Quando essas informações são definidas antes da instalação, o script de instalação detecta 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 devido a políticas de segurança ou por causa de alguma ferramenta de monitoramento de segurança, deverá adicioná-lo novamente. Você precisa preservar a configuração do sudoers, pois algumas operações do Unified Manager exigem esses privilégios de sudo.

As políticas de segurança do seu ambiente não devem restringir os 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 ao fazer login como o usuário umadmin após a instalação.

```
sudo systemctl status ocie
```

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

Passos

1. Faça login no servidor como usuário raiz.
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 base de sua escolha:

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

4. Defina a senha do umadmin:

   ```
   passwd umadmin
   ```

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

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

Baixe o Active IQ Unified Manager

Você precisa baixar o arquivo do Unified Manager `.zip` no 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.

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

Passos

1. Faça login no site de suporte da NetApp e acesse a página de download do Unified Manager:

   "NetApp site de suporte"

2. Selecione a versão necessária do Unified Manager e aceite o contrato de licença do usuário final.

3. Baixe o arquivo de instalação do Unified Manager para Linux e salve o `.zip` arquivo em um diretório no sistema de destino.

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

4. Verifique o checksum para garantir a integridade do software baixado.
5. Se você baixou o certificado de assinatura de código e a assinatura digital, pode 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>
     ```

     - Em que **AIQUM-RHEL-CLIENT-INTER-ROOT.pem** é o arquivo que contém o certificado de assinatura de código.
   - Este comando verifica a assinatura do arquivo de instalação:

     ```
     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 de instalação é seguro para uso.

Instale o Active IQ Unified Manager no Red Hat Enterprise Linux

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

Antes de começar

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

  Consulte "Requisitos de hardware do sistema".

  Consulte "Requisitos de software e instalação do Linux".

- Você deve ter baixado o arquivo do Unified Manager `.zip` do site de suporte da NetApp para o sistema de destino.
- Você deveria ter verificado a integridade do arquivo `.zip` baixado.
- Você precisa ter um navegador web compatível.

- Seu software de emulação de terminal deve ter a função de rolagem ativada.

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

Passos

1. Faça 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 o software e a versão
OpenJDK versão 17.0.14+6	`java -version`
O MySQL 8.4.10 Community Edition	`rpm -qa
grep -i mysql`	O 7-Zip

3. Se a versão do MySQL instalada for anterior à MySQL 8.4.10 Community Edition, digite o seguinte comando para desinstalá-lo:

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

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

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

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

   Os módulos necessários `.rpm` para o 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 nem 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 possui uma assinatura válida do Red Hat Enterprise Linux e se tem acesso aos repositórios de software necessários. Caso o script identifique algum problema, você deverá corrigi-lo antes de instalar o Unified Manager.

   Em um sistema Red Hat Enterprise Linux 8, se você tiver repositórios internos com JDK 17, OpenJDK, 7-zip e outros pacotes de software fornecidos pelo repositório AppStream, você deverá desativar 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 precisar baixar manualmente os pacotes necessários para a sua instalação. Se o seu sistema tiver acesso à internet e todos os pacotes necessários estiverem disponíveis, vá para a etapa 8. Para sistemas que não estão conectados à internet ou que não utilizam 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 “Installing:” são os pacotes disponíveis no diretório atual, e os itens na seção “Installing for dependencies:” 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 --downloaddir=.`

   > Como o plug-in “yum-plugin-downloadonly” nem sempre está habilitado em sistemas Red Hat Enterprise Linux, você pode precisar ativar 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 raiz ou usando `sudo`, execute o seguinte comando para instalar o software:

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

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

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

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

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

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

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

10. Depois que as mensagens de instalação forem concluídas, role a tela para trás pelas mensagens até ver a mensagem em que o sistema exibe um endereço IP ou URL para a interface do 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. Anote 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 base personalizado antes de instalar o Unified Manager, então você deve especificar o shell de login do usuário umadmin:

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

Acesse a interface 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.

Saiba mais sobre os usuários criados durante a instalação do Active IQ Unified Manager

Ao instalar o Unified Manager no Red Hat Enterprise Linux, os seguintes usuários são criados pelo Unified Manager e por utilitários de terceiros: umadmin, jboss e mysql.

- **umadmin**

  Usado para fazer login no Unified Manager pela primeira vez. Este usuário tem a função de usuário “Application Administrator” atribuída e está configurado como o tipo “Maintenance User”. Este usuário é criado pelo Unified Manager.

- **jboss**

  Usado para executar serviços do Unified Manager relacionados ao utilitário JBoss. O Unified Manager cria este usuário.

- **mysql**

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

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

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

Alterar a senha do JBoss no Active IQ Unified Manager

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

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

Passos

1. Faça login como usuário raiz no sistema.
2. Interrompa os serviços do Unified Manager inserindo os seguintes comandos na ordem apresentada:

   ```
   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, insira a nova senha do JBoss e, em seguida, insira-a uma segunda vez para confirmação.

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

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

6. Após todos os serviços serem iniciados, você poderá fazer login na interface do usuário do Unified Manager.

Atualizar o Unified Manager no Red Hat Enterprise Linux

Atualize o Active IQ 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 emparelhado 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, em seguida, configurar uma nova conexão do Workflow Automation após realizar as atualizações. Se você estiver atualizando apenas um dos produtos, deverá fazer login no Workflow Automation após a atualização e verificar se ele ainda está obtendo dados do Unified Manager.

Utilize o caminho de atualização compatível para as versões do Active IQ 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 permitem uma atualização direta para versões posteriores. As atualizações do Unified Manager são limitadas ao modelo N-2. Isso significa que você só pode atualizar para as duas versões seguintes em todas as plataformas. Por exemplo, você só pode atualizar para o Unified Manager 9.18 a partir do Unified Manager 9.14 e do Unified Manager 9.16.

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

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

Exemplo de caminho de atualização:

1. Atualização 9.11 → 9.13
2. Atualização 9.13 → 9.14
3. Atualização 9.13 → 9.16
4. Atualização da versão 9.14 ou 9.16 para a versão 9.18

Para obter mais informações sobre a matriz de caminho de atualização, consulte isto "artigo da Knowledge Base (KB)".

Atualize o Active IQ Unified Manager

Você pode atualizar do Unified Manager 9.14 ou 9.16 para 9.18 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.

  Consulte "Requisitos de hardware do sistema".

  Consulte "Requisitos de software e instalação do Linux".

- Você precisa ter uma assinatura do Red Hat Enterprise Linux Subscription Manager.

- Você deve instalar ou atualizar para a versão correta do OpenJDK antes de atualizar o Unified Manager.

  Consulte "Atualizando o JRE no Linux".

- Você deve instalar ou atualizar para a versão correta do 7-zip antes de atualizar o Unified Manager. Consulte "Configure o pacote de software 7-zip".
- Para evitar perda de dados, você deve ter criado um backup do banco de dados do Unified Manager caso ocorra algum problema durante a atualização. NetApp recomenda que você mova o arquivo de backup do `/opt/netapp/data` diretório para um local externo.
- Durante a atualização, talvez você seja 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. Ao confirmar, os dados históricos de desempenho serão apagados após 6 meses.
- Você deve ter concluído todas as operações em andamento, pois o Unified Manager fica indisponível durante o processo de atualização.
- O MySQL Community Edition é atualizado automaticamente durante a atualização do Unified Manager. Se a versão do MySQL instalada no seu sistema for anterior à 8.4.10, o processo de atualização do Unified Manager atualizará automaticamente o MySQL para 8.4.10.

Passos

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

   Consulte "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 softwares instalados que possam entrar em conflito com a atualização:

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

   O script de pré-instalação verifica se o sistema possui uma assinatura válida do Red Hat Enterprise Linux e se tem acesso aos repositórios de software necessários. Caso o script identifique algum problema, você deverá corrigi-lo e prosseguir com a atualização.

   Se forem detectados pacotes ausentes, execute os passos mencionados em "Etapas adicionais a serem executadas para pacotes ausentes". Se não houver pacotes ausentes, continue com os próximos passos.

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 que são executados neles. Além disso, o script de atualização verifica se há configurações do sistema ou softwares instalados que possam 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 o *net-snmp*, antes de atualizar o Unified Manager, a dependência do MySQL poderá desinstalar o pacote durante a atualização. Você precisará reinstalar manualmente o pacote para continuar a usá-lo.

7. Após a conclusão da atualização, role a tela para trás nas mensagens até encontrar a mensagem que exibe um endereço IP ou URL para a interface web do Unified Manager, o nome de 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 a senha que você definiu anteriormente.

Etapas adicionais a serem executadas para pacotes ausentes

Se forem detectados pacotes ausentes no seu site durante a atualização, 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 pacotes necessários ausentes e fazer o download desses pacotes.

> Esses passos devem ser executados após o passo *5* do procedimento principal. Este procedimento atualiza o Unified Manager, e você não precisa executar nenhum passo adicional para a atualização.

1. Veja a lista de pacotes disponíveis e indisponíveis:

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

   Os itens na seção “Installing:” são os pacotes disponíveis no diretório atual, e os itens na seção “Installing for dependencies:” 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 --downloaddir=.
   ```

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

   Como o plug-in “yum-plugin-downloadonly” nem sempre está habilitado em sistemas Red Hat Enterprise

Linux, pode ser necessário ativar a funcionalidade para baixar um pacote sem instalá-lo:

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

3. Copie os pacotes baixados para o diretório em que você descompactou o pacote 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 os seguintes 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 compatível para iniciar a interface da Web do Unified Manager e, em seguida, faça login usando o mesmo nome de usuário de manutenção (umadmin) e a senha que você definiu anteriormente.

Atualize o sistema operacional host Red Hat Enterprise Linux para o Active IQ Unified Manager

Se você instalou o Unified Manager em um sistema Red Hat Enterprise Linux 7.x e precisa atualizar para o Red Hat Enterprise Linux 8.x, siga um dos procedimentos listados neste tópico. Em ambos os casos, você deve criar um backup do Unified Manager no sistema Red Hat Enterprise Linux 7.x e, em seguida, restaurar o backup em um sistema Red Hat Enterprise Linux 8.x. Observe que as versões suportadas do Red Hat Enterprise Linux são de 8.0 a 8.10.

A diferença entre as duas opções listadas abaixo é que, em um caso, você está realizando a restauração do Unified Manager em um novo servidor 8.x e, no outro caso, está realizando 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, de forma que o Unified Manager fique offline pelo menor tempo possível. Lacunas nos dados coletados aparecem na UI do Unified Manager durante o período em que o sistema Red Hat Enterprise Linux 7.x fica desligado e antes de o novo Red Hat Enterprise Linux 8.x ser iniciado.

Consulte "Gerenciamento de 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 sobressalente no qual possa instalar o software Red Hat Enterprise Linux 8.x para poder realizar 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.

   Consulte "Requisitos de software e instalação do 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.

Consulte "Instalando o Unified Manager no Linux".

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

3. No sistema Red Hat Enterprise Linux 7.x, no menu Administração da interface da Web, crie um backup do Unified Manager e, em seguida, copie o arquivo de backup (`.7z` arquivo .backup) e o conteúdo do diretório do repositório do banco de dados (`/database-dumps-repo` subdiretório .db) 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` do local externo para `/opt/netapp/data/ocum-backup/` e os arquivos do repositório de banco de dados para o subdiretório `/database-dumps-repo` no diretório `/ocum-backup`.
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. Digite o endereço IP ou URL no seu navegador para iniciar a interface da web do Unified Manager e, em seguida, faça login no sistema.

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

Atualizando o sistema operacional do host no mesmo servidor

Siga estes passos se você não tiver um sistema sobressalente no qual possa instalar o software Red Hat Enterprise Linux 8.x.

1. No menu Administração da interface web, crie um backup do Unified Manager e, em seguida, 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 apague completamente o sistema.
3. Instale e configure o software Red Hat Enterprise Linux 8.x no mesmo sistema.

   Consulte "Requisitos de software e instalação do 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.

   Consulte "Instalando o Unified Manager no Linux".

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

5. Copie o arquivo de backup (`.7z` do local externo para `/opt/netapp/data/ocum-backup/` e os arquivos do repositório de banco de dados para o subdiretório `/database-dumps-repo` no diretório `/ocum-backup`.

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. Digite o endereço IP ou URL no seu navegador para iniciar a interface da web do Unified Manager e, em seguida, faça login no sistema.

Atualize produtos de terceiros após a instalação do Unified Manager

Atualize produtos de terceiro após instalar o Active IQ Unified Manager

Você pode atualizar produtos de terceiros, como o JRE, mesmo 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 quando for mais conveniente para você.

Atualize o OpenJDK no Linux para o Active IQ Unified Manager

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

Antes de começar

Você precisa ter privilégios de administrador (root) no sistema Linux em que o Unified Manager está instalado.

Você pode atualizar versões do OpenJDK dentro das 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. Faça login como usuário raiz na máquina host do Unified Manager.
2. Faça o download da versão apropriada do OpenJDK (64 bits) para o sistema de destino.
3. Interrompa os serviços do Unified Manager:

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

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

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

Reinicie o Active IQ Unified Manager

Pode ser necessário reiniciar o Unified Manager após efetuar alterações de configuração.

Antes de começar

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

Passos

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

```
systemctl stop ocieau

systemctl stop ocie

systemctl stop mysqld
```

3. Inicie os serviços do MySQL e do 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 Active IQ Unified Manager

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

Antes de começar

- Você precisa ter acesso de usuário raiz ao servidor do qual deseja remover o Unified Manager.
- O Security-Enhanced Linux (SELinux) deve ser desativado no sistema Linux. Altere o modo de execução do SELinux para “Permissive” usando o `setenforce 0` comando.
- Todos os clusters (fontes de dados) devem ser removidos do servidor Unified Manager antes da remoção do 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. Faça login como usuário raiz 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 RPM associados da NetApp. Ela não remove os módulos de software necessários, como Java, MySQL e 7zip.

3. **Opcional:** Se for apropriado, remova os módulos de software de suporte, como Java, MySQL e 7zip:

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

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

Remova o usuário umadmin personalizado e o grupo de manutenção do Active IQ Unified Manager

Se você criou um diretório base personalizado para definir seu próprio usuário umadmin e sua 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 de forma personalizada nem uma conta de manutenção. Você deve excluir esses itens manualmente.

Passos

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

```
userdel umadmin
```

3. Exclua o grupo de manutenção:

```
groupdel maintenance
```

Instale o Unified Manager em sistemas Windows

Introdução ao Active IQ Unified Manager

Saiba mais sobre o Active IQ Unified Manager

O Active IQ Unified Manager (formerly OnCommand Unified Manager) permite que você monitore e gerencie a integridade e o desempenho dos seus sistemas de storage 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 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

"NetApp Ferramenta de Matriz de Interoperabilidade"

Saiba o que o servidor Active IQ Unified Manager faz

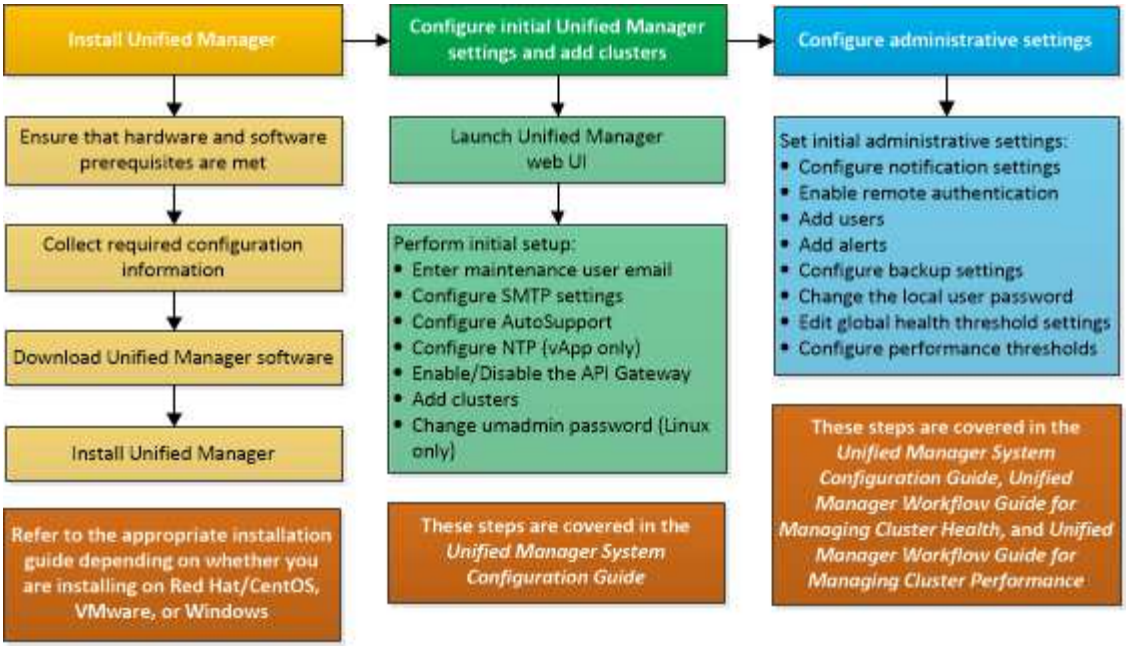
A infraestrutura do servidor do Unified Manager consiste em uma unidade de coleta de dados, um banco de dados e um servidor de aplicativos. Ela fornece serviços de infraestrutura como descoberta, monitoramento, controle de acesso baseado em funções (RBAC), auditoria e registro em log.

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

Saiba mais sobre a sequência de instalação do Active IQ Unified Manager

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

Certifique-se de que o servidor atenda aos requisitos de instalação do Active IQ Unified Manager

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

NetApp não oferece suporte a nenhuma modificação no código do aplicativo o Unified Manager. Se você precisar aplicar alguma medida de segurança ao servidor do Unified Manager, deverá fazer essas alterações no sistema operacional em que o Unified Manager está instalado.

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

"Suporte para medidas de segurança aplicadas ao Active IQ Unified Manager para o Clustered Data ONTAP"

Informações relacionadas

"NetApp Ferramenta de Matriz de Interoperabilidade"

Compreenda a infraestrutura virtual e os requisitos de hardware para o Active IQ Unified Manager

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

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

Configuração de hardware	Configurações recomendadas
RAM	12 GB
Processadores	4 CPUs
Capacidade de ciclos da CPU	9572 MHz no total (requisito mínimo de 9572 MHz)
Espaço livre em disco	150 GB, cuja capacidade é alocada da seguinte forma: • 100 GB de espaço de disco para o diretório de instalação • 50 GB de espaço de disco para o diretório de dados do MySQL

O Unified Manager pode ser instalado em sistemas com pouca memória, mas os 12 GB de RAM recomendados garantem que haja memória suficiente para um desempenho ideal e para que o sistema possa acomodar clusters e objetos de storage adicionais à medida que sua configuração cresce. Você não deve definir limites de memória na máquina virtual em que o Unified Manager está implantado nem habilitar recursos (por exemplo, ballooning) que impeçam o software de utilizar a memória alocada no sistema.

Além disso, existe 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 limites de nós, recomendações de CPU e memória, consulte "o Guia de Práticas Recomendadas do Unified Manager".

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

Requisito para uso dedicado

O sistema físico ou virtual no qual você instala o Unified Manager deve ser usado exclusivamente para o Unified Manager e não deve ser compartilhado com outros aplicativos. 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 em um destino remoto. A melhor prática é identificar um local remoto externo ao sistema host do Unified Manager que tenha no mínimo 150 GB de espaço.

Requisitos para conectividade de host

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

Você pode usar o nome do host (ou o endereço IP do host) para acessar a interface web do produto. Se você configurou um endereço IP estático para sua rede durante a implantação, então designou um nome para o host da rede. Se você configurou a rede usando DHCP, deve 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 o endereço IP, sua configuração de rede precisa resolver

esse nome curto para um FQDN válido.

Compreenda os requisitos de software e instalação do Windows para o Active IQ Unified Manager

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

Software do sistema operacional

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

- O Microsoft Windows Server 2019 Standard and Datacenter Edition
- O Microsoft Windows Server 2022 Standard and Datacenter Edition

O Unified Manager é compatível com sistema operacional Windows de 64 bits nos seguintes idiomas:

- Inglês
- Japonês
- Chinês simplificado

Consulte a Matriz de Interoperabilidade para obter a lista completa e mais atualizada das versões do Windows compatíveis.

"mysupport.netapp.com/matrix"

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 exclusivamente 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 normas da empresa. Você deve desativar o software antivírus antes de instalar o Unified Manager para evitar falhas na instalação.

Software de terceiros

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

- Pacotes redistribuíveis do Microsoft Visual C++ para Visual Studio 2015 versão 14.29.30133.0
- MySQL Community Edition versão 8.4.10
- Python 3.13.3
- OpenJDK versão 17.0.15+6
- 7-zip versão 25.01 ou posterior

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

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

- Está utilizando a porta padrão.
- Os bancos de dados de exemplo não estão instalados.
- O nome do serviço é “MYSQL84”.

O Unified Manager é implantado em um servidor web WildFly. O WildFly 27.0.1.Final é fornecido e configurado juntamente com o Unified Manager.

> Você deve encerrar uma instância em execução do Unified Manager antes de atualizar qualquer software de terceiro. Após a conclusão da instalação do software de terceiro, você poderá reiniciar o Unified Manager.

Requisitos de instalação

- O Microsoft .NET 4.5.2 ou superior deve estar instalado.
- O `temp` diretório deve ser configurado com 2 GB de espaço de 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 de disco na unidade do Windows para o armazenamento em cache dos arquivos MSI do Unified Manager.
- O Microsoft Windows Server no qual você deseja instalar o Unified Manager deve ser configurado com um domínio totalmente qualificado (FQDN), de modo que `ping` as respostas ao nome do host e ao FQDN sejam bem-sucedidas.
- Você deve desativar o serviço de publicação na Web do Microsoft IIS e garantir que as portas 80 e 443 estejam livres.
- Você deve garantir que a configuração “Windows Installer RDS Compatibility” do Host da Sessão de Área de Trabalho Remota esteja desativada durante a instalação.
- A porta UDP 514 deve estar livre e não deve ser usada por nenhum outro serviço.
- Você deve desativar todos os softwares antivírus do seu sistema antes de instalar o Unified Manager. Após a conclusão da instalação, certifique-se de excluir manualmente os seguintes caminhos da verificação do 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 do MySQL, por exemplo, `C:\ProgramData\MySQL\MySQLServerData`

Utilize navegadores compatíveis no Active IQ Unified Manager

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

A Interoperability Matrix contém a lista de versões de navegadores suportadas.

"mysupport.netapp.com/matrix"

Em todos os navegadores, desativar 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, também deve verificar a lista de navegadores compatíveis com o IdP.

Compreenda os requisitos de protocolo e porta para o Active IQ Unified Manager

As portas e os protocolos necessários permitem a comunicação entre o servidor do Unified Manager e os sistemas de armazenamento gerenciados, os 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 web do Unified Manager, pois as portas padrão são sempre utilizadas. Por exemplo, como o Unified Manager sempre tenta ser executado 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.
A interface do usuário da Web do Unified Manager e programas que usam APIs	HTTPS	443	Utilizado para acessar com segurança a interface do usuário da web do Unified Manager ou para fazer chamadas de API; as chamadas de API só podem ser feitas usando HTTPS.
Console de manutenção	SSH/SFTP	22	Utilizado 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.
Syslog	UDP	514	Utilizado para acessar mensagens EMS baseadas em assinatura dos sistemas ONTAP e para criar eventos com base nessas mensagens.

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

A porta padrão do MySQL, 3306, é restrita apenas ao localhost durante a instalação do Unified Manager em sistemas Windows. Após a conclusão da instalação, habilite o firewall para restringir o acesso à porta 3306 do MySQL. Isso não afeta nenhum cenário de atualização, em que a configuração anterior é mantida. Essa configuração pode ser modificada, e a conexão pode ser disponibilizada para outros hosts usando a `Control access to MySQL port 3306` opção no console de manutenção. Para obter informações, consulte "Opções adicionais do 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 obter mais informações, consulte "Configurando o Active IQ Unified Manager".

Conexões do servidor do Unified Manager

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

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

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

Destino	Protocolo	Porta	Descrição
Sistema de storage	HTTPS	443/TCP	Utilizado para monitorar e gerenciar sistemas de armazenamento.
Sistema de storage	NDMP	10000/TCP	Usado em determinadas operações de restauração de Snapshot.
AutoSupport servidor	HTTPS	443	Utilizado para enviar informações do AutoSupport. Requer 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	Utilizado para comunicação LDAP segura.	Servidor de e-mail
SMTP	25	Utilizado para enviar e-mails de notificação de alerta.	Remetente de trap SNMP
SNMPv1 ou SNMPv3	162/UDP	Usado para enviar notificações de alerta por traps SNMP.	Servidor do provedor de dados externo
TCP	2003	Usado para enviar dados de desempenho a um provedor de dados externo, como o Graphite.	Servidor NTP
NTP	123/UDP	Utilizado para sincronizar a hora no servidor Unified Manager com um servidor de horário NTP externo. (apenas para sistemas VMware)	Broker AMQP QPID
TCP/IP	56072	Usado para comunicação interna de mensagens.	Broker AMQP QPID
WebSocket sobre TCP	56080	Usada para escutar nesta porta mensagens recebidas do ONTAP (cloud agent).	Broker AMQP QPID

Destino	Protocolo	Porta	Descrição
WebSocket sobre TCP	56443	Usada para escutar nesta porta as mensagens recebidas do ONTAP (cloud agent). A comunicação por esta porta oferece suporte à criptografia fornecida por TLS ou SSL.	Syslog

Preencha a planilha no Active IQ Unified Manager

Antes de instalar e configurar o Unified Manager, você deve ter informações específicas sobre o seu ambiente prontamente disponíveis. Você pode registrar essas 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
Nome de domínio totalmente qualificado do host	
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.

Configuração	Seu valor
Endereço de e-mail do usuário de manutenção	
Nome do host do servidor SMTP ou endereço IP	
Nome de usuário SMTP	
Senha SMTP	
Porta SMTP	25 (Valor padrão)
E-mail a partir do qual as notificações de alerta são enviadas	

Configuração	Seu valor
Nome do host ou endereço IP do servidor de autenticação	
Nome do administrador do Active Directory ou nome diferenciado de vinculação LDAP	
Senha do Active Directory ou senha de bind LDAP	
Nome diferenciado base do servidor de autenticação	
URL do provedor de identidade (IdP)	
Metadados do provedor de identidade (IdP)	
Endereços IP do host de destino de traps SNMP	
Porta SNMP	

Informações do cluster

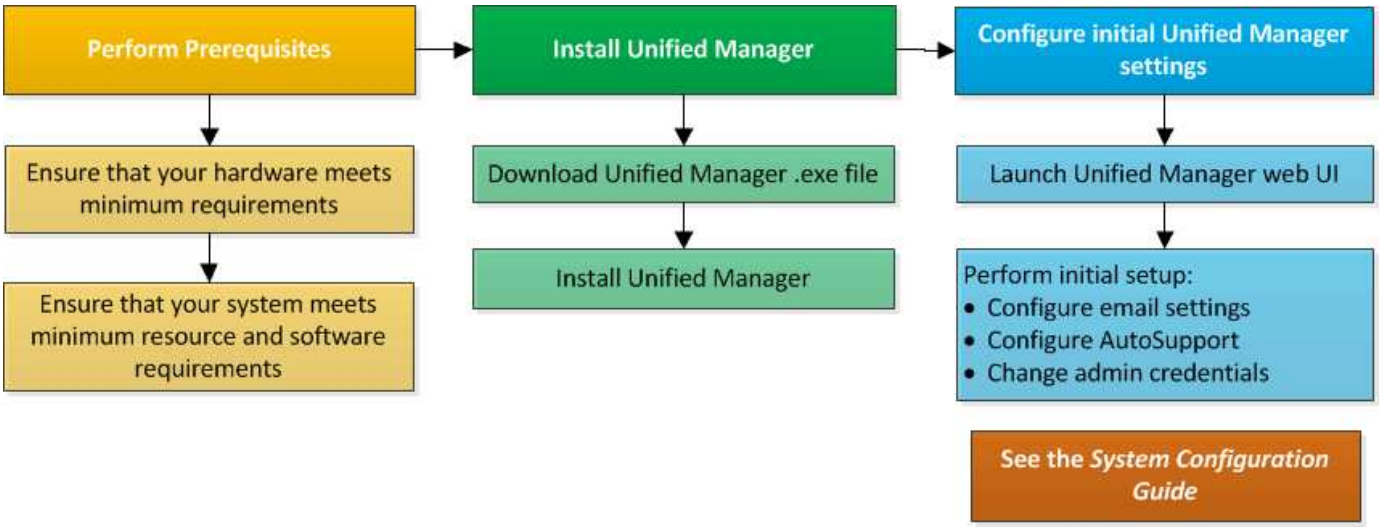
Os detalhes dos sistemas de armazenamento que você gerencia usando o Unified Manager.

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

Instalar, atualizar e remover o software Unified Manager

Saiba mais sobre o processo de instalação do Active IQ Unified Manager no Windows

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

Instale o Active IQ Unified Manager no Windows

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

Antes de começar

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

  Consulte "Requisitos de hardware do sistema".

  Consulte "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 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 precisa ter um navegador da web compatível.
- A senha do usuário de manutenção do Unified Manager deve ter entre 8 e 20 caracteres e conter letras maiúsculas ou minúsculas, números e caracteres especiais.
- Os seguintes caracteres especiais não são permitidos na string de senha para o usuário de manutenção ou para o usuário raiz do MySQL: " ' ` % , = & < > | ^ \ / ( ) [ ] ;:

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

Passos

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

   "NetApp site de suporte"

3. Selecione a versão necessária do Unified Manager e aceite o contrato de licença do usuário final.
4. Baixe o arquivo de instalação do Unified Manager para Windows ou o arquivo zip para um diretório de destino no sistema Windows.
5. Se necessário, extraia o arquivo zip 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 instala como parte da instalação.

7. Clique em **Avançar**.
8. Insira o nome de usuário e a senha para criar o usuário de manutenção.
9. No assistente de conexão com o banco de dados, insira a senha de 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 Ready to Install Shield, clique em **Install**.
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 do 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 do MySQL

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

- Diretório Java

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

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

  Este é o diretório onde todos os dados gerados pela aplicação são armazenados. Isso inclui logs, pacotes

de suporte, backup e todos os outros dados adicionais. Exemplo: `C:\ProgramData\NetApp\OnCommandAppData\`

Você pode acessar a interface da Web para realizar a configuração inicial do Unified Manager, conforme descrito no "Configurando o Active IQ Unified Manager".

Realize uma instalação não assistida do Active IQ 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 de chave-valor.

Passos

1. Faça 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	`ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qn /l*v CompletePathForLogFile"`
	
	Exemplo:
	
	`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"`

Opção	Instruções

Se os pacotes de terceiro não estiverem instalados	`ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qr /l*v CompletePathForLogFile"`
	
	Exemplo:
	
	`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"`

A `/qr`opção ativa o modo silencioso com uma interface de usuário reduzida. Uma interface de usuário básica é exibida, mostrando o progresso da instalação. Você não precisa inserir informações. Se pacotes de terceiro, como JRE, MySQL e 7zip, não estiverem pré-instalados, você deverá usar a `/qr`opção. A instalação falhará se a `/qn`opção for usada em um servidor onde pacotes de terceiro não estão instalados.

A `/qn` opção ativa o modo silencioso, sem interface de usuário. Nenhuma interface de usuário nem detalhes são exibidos durante a instalação. Você não deve usar a `/qn` opção quando os pacotes de terceiro não estiverem instalados.

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

   `https://IP address`

Altere a senha do JBoss no Windows no Active IQ Unified Manager

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

Antes de começar

- Você deve ter privilégios de administrador do Windows no sistema em que o Unified Manager está instalado.
- Você deve ter a senha do usuário raiz do MySQL.
- Você deverá conseguir acessar o script fornecido pela NetApp `password.bat` no diretório

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

Passos

1. Faça 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 do NetApp Active IQ (Ocie-au)
   - Serviço NetApp Active IQ Management Server (Oncommandsvc)
3. Execute o `password.bat` script para iniciar o processo de alteração de senha:

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

4. Quando solicitado, insira a senha do usuário raiz do MySQL.
5. Quando solicitado, insira a nova senha de usuário do JBoss e, em seguida, insira-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, uma letra 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 NetApp Active IQ Management Server (Oncommandsvc)
   - Serviço de aquisição do NetApp Active IQ (Ocie-au)
7. Após todos os serviços serem iniciados, você poderá fazer login na interface do usuário do Unified Manager.

Utilize o caminho de atualização compatível para as versões do Active IQ 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 permitem uma atualização direta para versões posteriores. As atualizações do Unified Manager são limitadas ao modelo N-2. Isso significa que você só pode atualizar para as duas versões seguintes em todas as plataformas. Por exemplo, você só pode atualizar para o Unified Manager 9.18 a partir do Unified Manager 9.14 e do Unified Manager 9.16.

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

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

Exemplo de caminho de atualização:

1. Atualização 9.11 → 9.13
2. Atualização 9.13 → 9.14
3. Atualização 9.13 → 9.16
4. Atualização da versão 9.14 ou 9.16 para a versão 9.18

Para obter mais informações sobre a matriz de caminho de atualização, consulte isto "artigo da Knowledge Base (KB)".

Atualize o Active IQ Unified Manager no Windows

Você pode atualizar o Unified Manager 9.14 ou 9.16 para 9.18 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.

  Consulte "Requisitos de hardware do sistema".

  Consulte "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 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 do MySQL instalada no seu sistema for anterior à 8.4.10, o processo de atualização do Unified Manager atualizará automaticamente o MySQL para 8.4.10. Você não deve executar uma atualização independente de uma versão anterior do MySQL para 8.4.10.
- Todos os clusters são suportados, exceto os ASA r2 Systems.
- 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 fazer login no site de suporte da NetApp.
- Para evitar perda de dados, você deveria ter criado um backup da máquina do Unified Manager caso ocorra algum problema durante a atualização.
- Você deve ter espaço de disco suficiente 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 adicionada caso não haja espaço livre.

- Durante a atualização, talvez você precise confirmar se deseja manter as configurações padrão anteriores para retenção de dados de desempenho por 13 meses ou alterá-las para 6 meses. Ao confirmar, os dados históricos de desempenho após 6 meses são apagados.
- 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 desativar todos os softwares de verificação de vírus no seu sistema antes de atualizar o Unified Manager.

Durante o processo de atualização, o Unified Manager ficará indisponível. Você deve concluir todas as operações em andamento antes de atualizar o Unified Manager.

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

Passos

1. Faça login no site de suporte da NetApp e acesse a página de download do Unified Manager:

   "NetApp site de suporte".

2. Selecione a versão necessária do Unified Manager e aceite o contrato de licença do usuário final.
3. Baixe o arquivo de instalação do o 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 o 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, em seguida, clique em **Avançar**.
5. Digite a senha de root do MySQL84 que foi definida durante a instalação e clique em **Avançar**.
6. Inicie a interface de usuário da web em uma nova janela em um navegador 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 do MySQL

Para realizar 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"`

Atualize produtos de terceiros

Atualize produtos de terceiro no Active IQ Unified Manager no Windows

Você pode atualizar produtos de terceiros, como o JRE, no Unified Manager quando ele estiver 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 quando for mais conveniente para você.

Atualize o OpenJDK no Windows para o Active IQ Unified Manager

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

Antes de começar

Você precisa ter privilégios de administrador do Windows no sistema em que 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. Faça login como usuário administrador na máquina host do Unified Manager.
2. Faça o download da versão apropriada do OpenJDK (64 bits) no site do OpenJDK para o sistema de destino.

   Por exemplo, faça o download do `jdk-17.0.15_windows-x64_bin.zip` arquivo de "a página Oracle Java SE 17 Archive Downloads".

   É necessário ter uma conta Oracle para baixar o arquivo. Se você não possui uma conta Oracle, acesse "a página de login da conta Oracle" para criar uma.

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

Desinstale produtos de terceiros no Active IQ Unified Manager

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

Desinstalar o Python

Passos

1. No **Painel de Controle** selecione **Programas** > **Programas e Recursos**.
2. Selecione Python na lista de programas.
3. Selecione **Desinstalar este programa**. Desinstale todas as versões do Python, exceto a 3.13.3. Certifique-se de manter a versão 3.13.3 do Python instalada.

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**.

Reinicie o Active IQ Unified Manager no Windows

Pode ser necessário reiniciar o Unified Manager após efetuar alterações de configuração.

Antes de começar

Você precisa ter privilégios de administrador do Windows.

Passos

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

Do…	Interrompa os serviços na seguinte ordem…
Linha de comando	a. `sc stop ocie-au` b. `sc stop Oncommandsvc`
O Microsoft Service Manager	a. Serviço de aquisição do NetApp Active IQ (Ocie-au) b. Serviço NetApp Active IQ Management Server (Oncommandsvc)

3. Inicie os serviços do Unified Manager:

Do…	Inicie os serviços na seguinte ordem…
Linha de comando	a. `sc start Oncommandsvc` b. `sc start ocie-au`
O Microsoft Service Manager	a. Serviço NetApp Active IQ Management Server (Oncommandsvc) b. Serviço de aquisição do NetApp Active IQ (Ocie-au)

Desinstale o Active IQ Unified Manager

Você pode desinstalar o Unified Manager usando o assistente de Programas e Recursos ou realizando uma desinstalação sem supervisão a partir da interface de linha de comando.

Antes de começar

- Você precisa ter privilégios de administrador do Windows.

- Todos os clusters (fontes de dados) devem ser removidos do servidor do Unified Manager antes da desinstalação do 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 pelo assistente de **Programas e Recursos**, siga estes passos:
     i. Acesse **Painel de Controle** > **Programas e Recursos**.
     ii. Selecione o Active IQ Unified Manager e clique em **Desinstalar**.
   - Se você desinstalar o Unified Manager pela linha de comando, siga estas etapas:
     i. Faça login na linha de comando do Windows usando privilégios de administrador.
     ii. 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 ativado no servidor e você estiver conectado como um usuário de domínio, deverá 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 da aplicação MySQL gerados pelo Unified Manager
   - Logs do aplicativo e conteúdo do diretório de dados do aplicativo

Execute tarefas de configuração e administração

Configurar o Active IQ Unified Manager

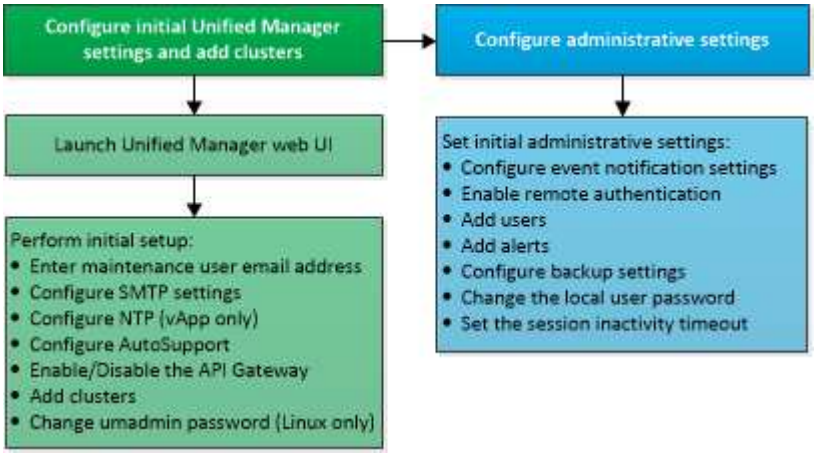
Saiba mais sobre como configurar o Active IQ Unified Manager

Após instalar o Active IQ Unified Manager (anteriormente o OnCommand Unified Manager), você deve concluir a configuração inicial (também chamada de assistente de primeira experiência) para acessar a interface de usuário da web. Em seguida, você pode realizar tarefas de configuração adicionais, como adicionar clusters, configurar a 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 configurações recomendadas que podem ser úteis para configurar sua nova instância ou que é bom conhecer antes de iniciar o monitoramento regular dos seus sistemas ONTAP.

Saiba mais sobre a sequência de configuração no Active IQ Unified Manager

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



Acesse a interface web no Active IQ Unified Manager

Após instalar o Unified Manager, você poderá 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 está acessando a interface de usuário da web, você deve fazer login como o usuário de manutenção (ou o usuário umadmin para instalações do Linux).
- Se você planeja permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o domínio totalmente qualificado (FQDN) ou o 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 aceitar o risco para continuar acessando ou instalar um certificado

digital assinado por uma Autoridade Certificadora (CA) para autenticação do servidor.

Passos

1. Inicie a interface web do Unified Manager no seu navegador usando a URL exibida no final da instalação. A URL é o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do servidor Unified Manager.

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

2. Faça 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 de usuário da web em uma hora, seu acesso ao sistema será bloqueado, e você precisará entrar em contato com o administrador do sistema. Isso se aplica somente a usuários locais.

Execute a configuração inicial da interface web do Active IQ Unified Manager

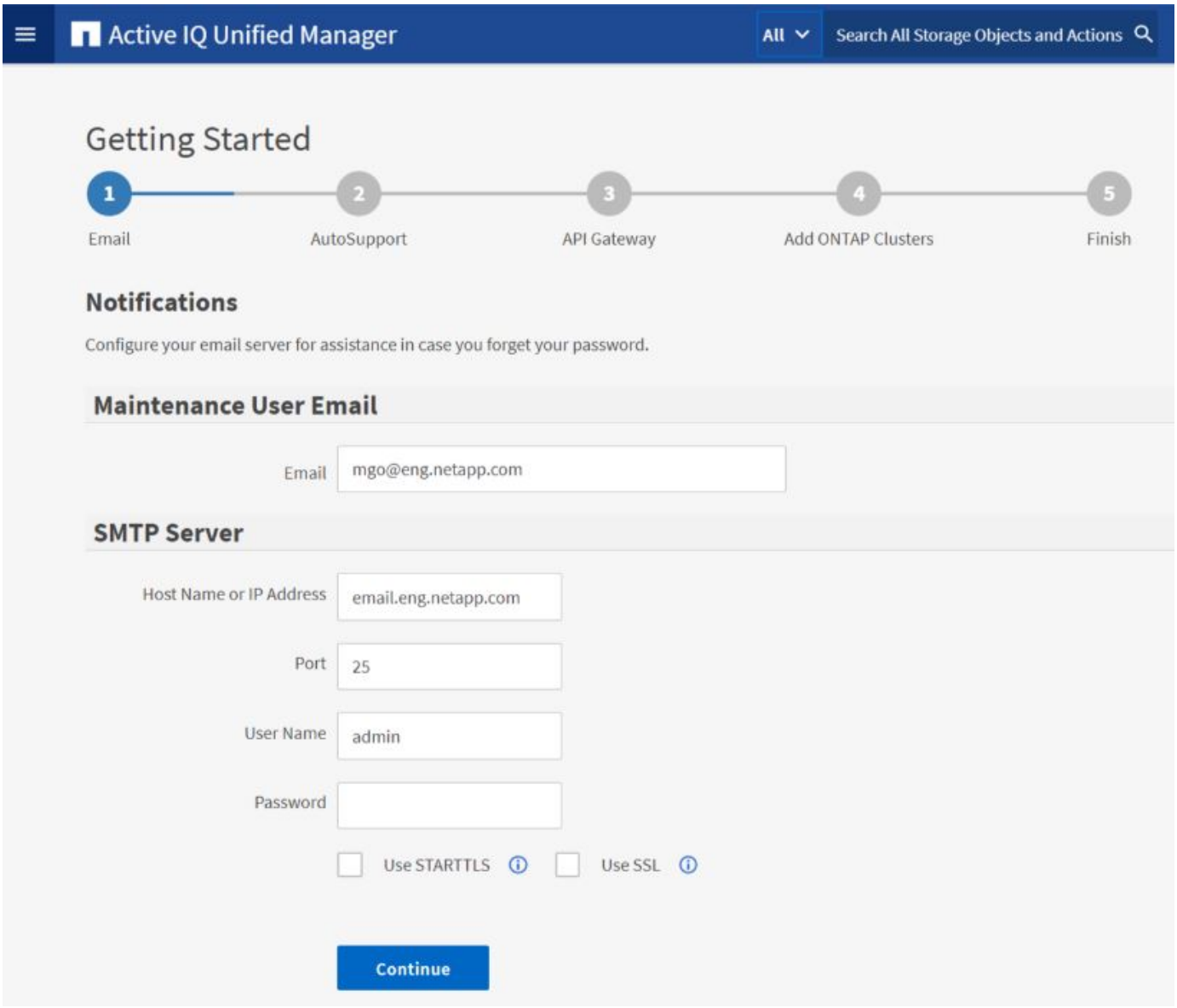
Para usar o Unified Manager, você deve primeiro configurar as opções de configuração inicial, incluindo o servidor NTP, o endereço de e-mail do usuário de manutenção, o host do servidor SMTP e a adição de clusters do ONTAP.

Antes de começar

Você deve ter realizado as seguintes operações:

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

A página Active IQ Unified ManagerGetting Started aparece somente quando você acessa a interface web pela primeira vez. A página abaixo é de uma instalação no VMware.



Se quiser alterar qualquer uma dessas opções posteriormente, você poderá selecionar sua escolha nas opções Gerais no painel de navegação à esquerda do Unified Manager. Observe que a configuração de NTP é exclusiva para instalações VMware e pode ser alterada posteriormente usando o console de manutenção do Unified Manager.

Passos

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

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

2. Na página AutoSupport, clique em **Agree and Continue** 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 desativar 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 Gateway de API, selecione se deseja usar o recurso Gateway de API que permite ao Unified Manager gerenciar os clusters do ONTAP que você planeja monitorar usando as APIs REST do ONTAP. Em seguida, clique em **Continuar**.

   Você pode ativar ou desativar essa configuração posteriormente na interface da web em **Geral** > **Configurações de recursos** > **Gateway de API**. Para obter mais informações sobre as APIs, consulte "Primeiros passos com as 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 o nome de usuário e as credenciais de senha; o usuário deve ter a função “admin”.

   Esta etapa é opcional. Você pode adicionar clusters posteriormente na interface de usuário da web em **Gerenciamento de armazenamento** > **Configuração de cluster**.

6. Na página de resumo, verifique se todas as configurações estão corretas e clique em **Concluir**.

A página de introdução é fechada e a página Dashboard do Unified Manager é exibida.

Adicionar clusters ao Active IQ Unified Manager

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

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter as seguintes informações:
  - O Unified Manager oferece suporte a clusters ONTAP locais, ao ONTAP Select e ao Cloud Volumes ONTAP.
  - Nome do host ou endereço IP de gerenciamento do 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 do cluster deve ser a LIF de gerenciamento do cluster da máquina virtual de armazenamento administrativa (SVM). Se você usar uma LIF de gerenciamento de nó, 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*, *amqp*, *console* e *http*.

  - O número da porta para conectar-se ao cluster usando o protocolo HTTPS (normalmente a porta 443)

- Você possui os certificados necessários:

  Certificado SSL (HTTPS): este certificado pertence ao Unified Manager. Um certificado SSL (HTTPS) autoassinado padrão é gerado com uma nova instalação do Unified Manager. NetApp recomenda que você o 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 como regenerar o certificado SSL, consulte "Gerando um certificado de segurança HTTPS".

  Certificado EMS: Este certificado pertence ao Unified Manager. Ele é usado durante a autenticação para notificações EMS recebidas do ONTAP.

  Certificados para comunicação TLS mútua: utilizados durante a comunicação TLS mútua entre o Unified Manager e o ONTAP. A autenticação baseada em certificado é habilitada para um cluster, dependendo da versão do ONTAP. Se o cluster que executa a versão do ONTAP for inferior a 9.5, a autenticação baseada em certificado não será habilitada.

  A autenticação baseada em certificado não é habilitada automaticamente para um cluster se você estiver atualizando uma versão mais antiga do Unified Manager. No entanto, você pode habilitá-la 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 pela interface de usuário da web, e a autenticação baseada em certificado é ativada automaticamente.
  - Você pode adicionar um cluster pela CLI do Unified Manager; a autenticação baseada em certificado não está habilitada por padrão. Se você adicionar um cluster usando a CLI do Unified Manager, precisará editar o cluster usando a interface do usuário do Unified Manager. Consulte "Comandos da CLI do Unified Manager suportados" para adicionar um cluster usando a CLI do Unified Manager.
  - Se a autenticação baseada em certificado estiver habilitada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurá-lo em outro servidor do Unified Manager em que o nome do host ou o endereço IP foi alterado, o monitoramento do cluster poderá falhar. Para evitar essa falha, edite e salve os detalhes do cluster. Para obter mais informações sobre como editar os detalhes do cluster, consulte "Editando clusters".

  +
  Certificados de cluster: Este certificado pertence ao ONTAP. Não é possível adicionar um cluster ao Unified Manager com um certificado expirado e, caso o certificado já tenha expirado, você deve regenerá-lo antes de adicionar o cluster. Para obter informações sobre a geração de certificados, consulte o artigo da base de conhecimento (KB) "Como renovar um certificado autoassinado do ONTAP na interface de usuário do System Manager".

- Você precisa ter espaço suficiente no servidor do Unified Manager. A adição de um cluster ao servidor não será possível se mais de 90% do espaço no diretório do banco de dados já estiver ocupado.

Para uma configuração do MetroCluster, você precisa adicionar os clusters local e remoto, e ambos devem estar configurados corretamente.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de cluster**.

2. Na página de Configuração do Cluster, clique em **Adicionar**.
3. Na caixa de diálogo Add Cluster, especifique os valores necessários, como o nome do host ou o endereço IP do cluster, o nome de usuário, a senha e o número da porta.

   Você pode alterar o endereço IP de gerenciamento do cluster de IPv6 para IPv4 ou de IPv4 para IPv6. O novo endereço IP será 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 Authorize Host, clique em **View Certificate** para visualizar as informações do certificado do cluster.
6. Clique em **Yes**.

   Após salvar os detalhes do cluster, você poderá visualizar o certificado para a comunicação TLS mútua de um cluster.

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

Após todos os objetos de um novo cluster serem 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. Esse recurso fornece a você mais de duas semanas de informações de desempenho de um cluster imediatamente após sua adição. 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 muito da CPU, recomenda-se que você adicione novos clusters de forma escalonada para que as sondagens da 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 referentes ao período ausente.

Se você receber uma mensagem de erro informando que não é possível adicionar o cluster, verifique se os relógios dos 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 o NTP ou um serviço similar.

Informações relacionadas

"Instalando um certificado HTTPS assinado e retornado por uma Autoridade Certificadora (CA)"

Configurar notificações

Configure o Active IQ Unified Manager para enviar notificações de alerta

Você pode configurar o Unified Manager para enviar notificações que alertem você sobre eventos em seu ambiente. Antes que as notificações possam ser enviadas, você deve configurar várias outras opções do Unified Manager.

Antes de começar

Você precisa ter a função de Application Administrator.

Após implantar o Unified Manager e concluir a configuração inicial, você deve considerar configurar seu ambiente para disparar alertas e gerar e-mails de notificação ou traps SNMP com base no recebimento de eventos.

Passos

1. "Configure as definições de notificação de eventos".

   Se você quiser que as notificações de alerta sejam enviadas quando determinados eventos ocorrerem em seu ambiente, será necessário configurar um servidor SMTP e fornecer um endereço de e-mail a partir do qual a notificação de alerta será enviada. Se você quiser usar traps SNMP, poderá 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, você deverá habilitar a autenticação remota.

3. "Adicionar servidores de autenticação".

   Você pode adicionar servidores de autenticação para que usuários remotos no 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 envio de notificações, adicionar os usuários que receberão as notificações, configurar as definições de rede e configurar as opções SMTP e SNMP necessárias para o seu ambiente, você poderá atribuir alertas.

Configure as definições de notificação de eventos no Active IQ Unified Manager

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

Antes de começar

Você precisa ter as seguintes informações:

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

  O endereço de e-mail aparece no campo “From” nas notificações de alerta enviadas. Se o e-mail não puder ser entregue por algum motivo, esse endereço de e-mail também será usado como destinatário para mensagens não entregues.

- Nome do host do servidor SMTP, nome de usuário e senha para acessar o servidor

- Nome do host ou endereço IP do host de destino do trap que receberá o trap SNMP, juntamente com a versão SNMP, a porta de saída do trap, a comunidade e outros valores de configuração SNMP necessários

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

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

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

   Notas:

   - Se o campo "De" estiver preenchido automaticamente com o endereço "ActiveIQUnifiedManager@localhost.com", você deve alterá-lo para um endereço de e-mail real e funcional para garantir que todas as notificações por e-mail sejam entregues com sucesso.
   - Caso o nome do host do servidor SMTP não possa ser resolvido, você pode 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 é exibida após clicar no botão **Salvar**. Verifique os detalhes do certificado e aceite-o para salvar as configurações de notificação.

   Você pode clicar no botão **Exibir detalhes do certificado** para visualizar os detalhes do certificado. Se o certificado atual 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.

Ative a autenticação remota no Active IQ Unified Manager

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 storage e dados.

Antes de começar

Você precisa ter a função de Application Administrator.

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

Você pode 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 via LDAP e LDAPS (Secure LDAP). O Unified Manager utiliza a porta 389 como padrão para comunicação não segura e a porta 636 como padrão para comunicação segura.

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

Passos

1. No painel de navegação à esquerda, 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 o tipo de autenticação…	Insira as seguintes informações…
Active Directory	• 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 de administrador • Nome diferenciado base (usando a notação LDAP apropriada)
Open LDAP	• Nome diferenciado de bind (na notação LDAP apropriada) • Senha de vinculação • Nome diferenciado base

Se a autenticação de um usuário do Active Directory demorar muito ou expirar, o servidor de autenticação provavelmente está demorando muito para responder. Desativar o suporte a 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**.

Desative grupos aninhados na autenticação remota no Active IQ Unified Manager

Se você tiver a autenticação remota habilitada, poderá desabilitar a autenticação de grupos aninhados para que somente usuários individuais, e não membros de grupos, 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 precisa ter a função de Application Administrator.
- Desativar grupos aninhados só se aplica ao uso do Active Directory.

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

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Marque a caixa de seleção para **Disable Nested Group Lookup**.
3. Clique em **Salvar**.

Configure os serviços de autenticação no Active IQ Unified Manager

Os serviços de autenticação permitem a autenticação de usuários remotos ou grupos remotos em um servidor de autenticação antes de conceder 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 precisa ter a função de Application Administrator.

Passos

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

Se você selecionar…	Então faça isso…
Active Directory	a. Digite o nome do administrador e a senha. b. Especifique o nome diferenciado base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, então o nome diferenciado base será **cn=ou,dc=domain,dc=com**.
O OpenLDAP	a. Insira o nome diferenciado de vinculação e a senha de vinculação. b. Especifique o nome diferenciado base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, então o nome diferenciado base será **cn=ou,dc=domain,dc=com**.

Se você selecionar…	Então faça isso…
Outros	a. Insira o nome diferenciado de vinculação e a senha de vinculação. b. Especifique o nome diferenciado base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, então o nome diferenciado base será **cn=ou,dc=domain,dc=com**. c. Especifique a versão do protocolo LDAP compatível com o servidor de autenticação. d. Insira o nome de usuário, a associação a grupos, o grupo de usuários e os atributos do membro.

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

3. Clique em **Salvar**.

Adicionar servidores de autenticação ao Active IQ Unified Manager

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

Antes de começar

- As informações a seguir 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 precisa ter a função de Application Administrator.

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 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 à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Ative ou desative a opção **Use secure connection**:

Se você quiser…	Então faça isso…
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 o endereço IP (IPv4 ou IPv6) do servidor. d. Na caixa de diálogo Authorize Host, clique em View Certificate. e. Na caixa de diálogo Exibir Certificado, verifique as informações do certificado e clique em **Fechar**. f. Na caixa de diálogo "Authorize Host", clique em **Yes**. Quando você ativa a opção **Use Secure Connection authentication**, o Unified Manager se comunica com o servidor de autenticação e exibe o certificado. O Unified Manager usa a porta 636 como porta padrão para comunicação segura e a porta 389 para comunicação não segura.
Desative-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, bem como os detalhes da porta. d. Clique em **Add**.

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

3. Realize um teste de autenticação para confirmar que você consegue autenticar usuários no servidor de autenticação que você adicionou.

Teste a configuração dos servidores de autenticação no Active IQ Unified Manager

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 nos seus servidores de autenticação e autenticando esse usuário ou grupo 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 remoto ou o grupo remoto.
- Você deve ter adicionado seus servidores de autenticação para que o servidor de gerenciamento possa procurar o usuário remoto ou o grupo remoto nesses servidores e autenticá-los.
- Você precisa ter a função de Application Administrator.

Se o serviço de autenticação estiver configurado para o Active Directory e se você estiver validando a autenticação de usuários remotos que pertencem ao grupo primário do servidor de autenticação, as informações sobre o grupo primário não serão exibidas nos resultados da autenticação.

Passos

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

   Se você estiver autenticando um grupo remoto, não deve inserir a senha.

Adicione alertas no Active IQ Unified Manager

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

Antes de começar

- Você precisa ter configurado as definições de notificação, como o endereço de e-mail do usuário, o servidor SMTP e o host de trap SNMP, para permitir que o servidor Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento for gerado.
- Você precisa saber os recursos e eventos para os quais deseja acionar o alerta, bem como os nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se você quiser que um script seja executado com base no evento, deve ter adicionado o script ao Unified Manager usando a página Scripts.
- Você precisa ter a função de Application Administrator ou Storage Administrator.

Além de criar um alerta na página de Configuração de Alertas, conforme descrito aqui, você pode criá-lo diretamente na página de detalhes do evento após receber um evento.

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
2. Na página Configuração de alertas, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar alerta, clique em **Nome** e insira um nome e uma descrição para o alerta.
4. Clique em **Recursos**, e selecione os recursos que deseja incluir ou excluir do alerta.

   Você pode definir um filtro especificando uma cadeia de texto no campo **Nome contém** para selecionar um grupo de recursos. Com base na cadeia de texto que você especificar, a lista de recursos disponíveis exibe apenas os recursos que correspondem à regra de filtro. A cadeia de texto que você especificar

diferencia maiúsculas de minúsculas.

Se um recurso estiver em conformidade com as regras de inclusão e exclusão que você especificou, a regra de exclusão tem precedência sobre a regra de inclusão, e o alerta não é gerado para eventos relacionados ao recurso excluído.

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



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

6. Clique em **Ações** e selecione os usuários que você deseja notificar, escolha a frequência de notificação, defina se um trap SNMP será enviado ao receptor de traps e atribua um script para executar 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, pois o endereço de e-mail modificado não estará mais vinculado ao 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 como adicionar um alerta

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

- Nome do alerta: HealthTest
- Recursos: inclui todos os volumes cujo nome contém “abc” e exclui todos os volumes cujo nome contém “xyz”
- Eventos: inclui todos os eventos críticos de saúde
- Ações: inclui "sample@domain.com", um script “Test” e o usuário deve ser notificado a cada 15 minutos

Execute as etapas a seguir na caixa de diálogo Add Alert:

Passos

1. Clique em **Nome** e digite **HealthTest** no campo **Nome do alerta**.
2. Clique em **Resources** e, na guia Include, selecione **Volumes** na lista suspensa.
   a. Digite **abc** no campo **Nome contém** para exibir os volumes cujo nome contém “abc”.
   b. Selecione **<<All Volumes whose name contains 'abc'>>** na área Recursos Disponíveis e mova-o para a área Recursos Selecionados.
   c. Clique em **Excluir**, digite **xyz** no campo **Nome contém** e, em seguida, clique em **Adicionar**.
3. Clique em **Eventos** e selecione **Crítico** no campo Severidade do evento.
4. Selecione **Todos os eventos críticos** na área Eventos correspondentes e mova-o para a área Eventos selecionados.
5. Clique em **Actions**, e digite **sample@domain.com** no campo Alert these users.

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 durante um período específico. Você deve determinar o horário a partir do qual a notificação do 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 no Active IQ Unified Manager

Você pode alterar a senha de login do seu usuário local para evitar possíveis riscos de segurança.

Antes de começar

Você precisa estar conectado como um usuário local.

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

Passos

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

   A opção **Change Password** não é exibida se você for um usuário remoto.

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

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

Defina o tempo limite de inatividade da sessão no Active IQ Unified Manager

Você pode especificar o valor de tempo limite de inatividade para o 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 precisa ter a função de Application Administrator.

Essa configuração afeta todas as sessões de usuários conectados.

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

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 isso…
Não defina um tempo limite para que a sessão nunca seja fechada automaticamente	No painel **Tempo limite de inatividade**, mova o botão deslizante para a esquerda (desativado) e clique em **Aplicar**.
Defina um número específico de minutos como o valor de tempo limite	No painel **Tempo limite de inatividade**, mova o botão deslizante para a direita (ativado), especifique o valor do tempo limite de inatividade em minutos e clique em **Aplicar**.

Defina o tempo limite da sessão usando a CLI no Active IQ Unified Manager

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. Por padrão, o tempo limite da sua sessão está definido para o valor máximo, que é de 4.320 minutos (72 horas). Isso significa que sua sessão termina automaticamente após 72 horas, mesmo se você estiver conectado e usando o Unified Manager.

Sobre esta tarefa

Você precisa ter a função de Application Administrator.

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

Passos

1. Faça login na CLI do Unified Manager digitando o `um cli login` comando. Use um nome de usuário e uma senha válidos para autenticação.
2. Digite o `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

Alterar o nome do host da máquina virtual do Active IQ 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 regenerar o certificado HTTPS.

Antes de começar

Para executar essas tarefas, você precisa estar conectado ao Unified Manager como usuário de manutenção ou ter a função de Application Administrator atribuída.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a interface do usuário da Web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, então você terá atribuído um nome ao 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 estiverem configurados corretamente, o nome do host “Unified Manager” será atribuído automaticamente e associado ao certificado de segurança.

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

Se você acessar a interface web usando o endereço IP em vez do nome do host, não precisará gerar um novo certificado caso altere 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 só entrará em vigor após a reinicialização da máquina virtual do Unified Manager.

Passos

1. Gere um certificado de segurança HTTPS

   Se você quiser usar o novo nome de host para acessar a interface da web do Unified Manager, será necessário gerar novamente o certificado HTTPS para associá-lo ao novo nome de host.

2. Reinicie a máquina virtual do Unified Manager

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

Gere um certificado de segurança HTTPS no Active IQ Unified Manager

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 para substituir o certificado existente.

Antes de começar

Você precisa ter a função de Application Administrator.

Pode haver vários motivos para regenerar o certificado, por exemplo, se você quiser valores melhores para o Nome distinto (DN), um tamanho de chave maior, um período de expiração mais longo ou se o certificado atual tiver expirado.

Se você não tiver acesso à interface web do Unified Manager, poderá regenerar o certificado HTTPS com os mesmos valores usando o console de manutenção. Ao regenerar os certificados, você pode definir o tamanho da chave e a duração de validade da chave. Se você usar a opção `Reset Server Certificate` no console de manutenção, um novo certificado HTTPS será criado e será válido por 397 dias. Este certificado terá uma chave RSA de 2048 bits.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.
2. Clique em **Regenerate HTTPS Certificate**.

   A caixa de diálogo "Regenerate HTTPS Certificate" é exibida.

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

Se você quiser…	Faça isso…
Gere novamente o certificado com os valores atuais	Clique na opção **Regenerar usando os atributos do certificado atual**.

Se você quiser…	Faça isso…
Gere o certificado usando valores diferentes	Clique na opção **Atualizar os atributos do certificado atual**. 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 variam de um mínimo de 1 dia a um máximo de 36.500 dias. Embora seja permitido um período de validade de 36500 dias, recomenda-se que você utilize um período de validade de no máximo 397 dias ou 13 meses. Isso porque, se você selecionar um período de validade superior a 397 dias e planejar exportar um CSR para este certificado e obtê-lo assinado por uma CA reconhecida, a validade do certificado assinado retornado a você pela CA será reduzida para 397 dias. • Você pode selecionar a caixa de seleção "Excluir informações de identificação local (ex.: localhost)" se quiser remover as informações de identificação local do campo Nomes Alternativos no certificado. Quando essa 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 ao visualizar o certificado HTTPS.

Reinicie a máquina virtual do Active IQ Unified Manager

Você pode reiniciar a máquina virtual a partir do 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 appliance virtual está ligado.

Você está conectado ao console de manutenção como o usuário de manutenção.

Você também pode reiniciar a máquina virtual a partir do vSphere usando a opção **Restart Guest**. Consulte a documentação da VMware para obter mais informações.

Passos

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

Altere o nome do host do Active IQ Unified Manager em sistemas Linux

Em algum momento, você poderá 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 os 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 raiz ao sistema Linux no qual o Unified Manager está instalado.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a interface da web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, então terá 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 pretender 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 prática recomendada é atualizar o certificado para que o nome do host no certificado corresponda ao nome real do host. O novo certificado só entrará em vigor depois que a máquina Linux for 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. Faça login como usuário raiz no sistema do Unified Manager que você deseja modificar.

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

   ```
   systemctl stop ocieau ocie mysqld
   ```

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

   ```
   hostnamectl set-hostname new_FQDN
   ```

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Gere novamente 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 reiniciar o serviço, verifique se o novo nome do host consegue dar ping em si mesmo:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Este comando deve retornar o mesmo endereço IP que você definiu 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
   ```

Ative e desative o gerenciamento de storage baseado em políticas no Active IQ Unified Manager

A partir do Unified Manager 9.7, você pode provisionar cargas de trabalho de storage (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 associação de políticas de QoS, mas, quando aplicada usando o Unified Manager, permite provisionar e gerenciar cargas de trabalho em todos os clusters que a sua instância do Unified Manager está monitorando.

Você precisa ter a função de Application Administrator.

Essa opção está habilitada por padrão, mas você pode desativá-la se não quiser provisionar e gerenciar cargas de trabalho usando o Unified Manager.

Quando ativada, esta opção fornece vários novos itens na interface de 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 storage de desempenho	Disponível em **Configurações** > **Políticas** > **Eficiência de storage**
Painéis que descrevem o desempenho atual da sua carga de trabalho e as IOPS da sua carga de trabalho	Disponível no painel de controle

Consulte a ajuda online do produto para obter mais informações sobre essas páginas e sobre 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 storage baseado em políticas escolhendo uma das seguintes opções:

Se você quiser…	Então faça isso…
Desativar o gerenciamento de storage baseado em políticas	No painel **gerenciamento de storage baseado em políticas**, mova o botão deslizante para a esquerda.
Habilitar o gerenciamento de storage baseado em políticas	No painel **gerenciamento de storage baseado em políticas**, mova o botão deslizante para a direita.

Configurar o Active IQ Unified Manager backup

Você pode configurar a funcionalidade de backup no Unified Manager por meio de um conjunto de etapas de configuração a serem executadas nos sistemas host e pelo console de manutenção.

Para obter informações sobre as etapas de configuração, consulte "Gerenciamento de operações de backup e restauração".

Gerenciar configurações de recursos

Saiba mais sobre as configurações de recursos no Active IQ Unified Manager

A página Configurações de recursos permite ativar e desativar recursos específicos no Active IQ Unified Manager. Isso inclui a criação e o gerenciamento de objetos de storage com base em políticas, a ativação do API Gateway e do Login Banner, o upload de scripts para gerenciar alertas, o encerramento automático de uma sessão da interface de usuário da web com base no tempo de inatividade e a desativação do recebimento de eventos da plataforma Active IQ.

A página Configurações de recursos está disponível apenas para usuários com a função

Administrador de Aplicativos.

Para obter informações sobre Scripts Upload, consulte "Ativar e desativar o upload de scripts".

Habilite o gerenciamento de storage baseado em políticas no Active IQ Unified Manager

A opção **Gerenciamento de storage baseado em políticas** permite o gerenciamento de storage com base em objetivos de nível de serviço (SLOs). Essa opção está habilitada por padrão.

Ao ativar esse recurso, você pode provisionar cargas de trabalho de storage nos clusters do 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 nas políticas de eficiência de storage atribuídos.

Você pode optar por ativar ou desativar esse recurso em **Geral** > **Configurações de recursos** > **gerenciamento de storage baseado em política**. Ao ativar esse recurso, as seguintes páginas ficam disponíveis para operação e monitoramento:

- Provisionamento (provisionamento de cargas de trabalho de storage)
- **Políticas** > **Níveis de Serviço de Desempenho**
- **Políticas** > **Eficiência de storage**
- 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 de controle**

Você pode usar as telas para criar níveis de serviço de desempenho e políticas de eficiência de storage, além de provisionar cargas de trabalho de storage. Você também pode monitorar as cargas de trabalho de storage que estão em conformidade com os níveis de serviço de desempenho atribuídos, bem como aquelas que não estão em conformidade. O painel Desempenho da Carga de Trabalho e IOPS da Carga de Trabalho também permite avaliar a capacidade e o desempenho (IOPS) totais, disponíveis e usados dos clusters em todo o seu data center, com base nas cargas de trabalho de storage provisionadas neles.

Após ativar esse recurso, você pode executar as APIs REST do Unified Manager para realizar algumas dessas funções em **Menu Bar** > **Help button** > **API Documentation** > categoria **storage-provider**. Como alternativa, você pode inserir o nome do host ou o 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 "Primeiros passos com as APIs REST do Active IQ Unified Manager".

Saiba mais sobre o recurso API Gateway no Active IQ Unified Manager

O recurso API Gateway permite que o Active IQ Unified Manager seja um plano de controle único a partir do qual você pode gerenciar múltiplos clusters ONTAP, sem precisar fazer login em cada um individualmente.

Você pode ativar esse recurso nas páginas de configuração que aparecem quando você faz login pela primeira vez no Unified Manager. Como alternativa, você pode ativar ou desativar esse recurso em **General** > **Feature Settings** > **API Gateway**.

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 usadas com as APIs REST do Unified Manager. No entanto, se você tiver um requisito empresarial específico para acessar as APIs do ONTAP e gerenciar recursos específicos que não são expostos ao Unified Manager, poderá habilitar o recurso API Gateway e executar as APIs do ONTAP. O gateway atua como um proxy para encapsular as solicitações de API, mantendo as solicitações de cabeçalho e corpo no mesmo formato das APIs do ONTAP. Você pode usar suas credenciais do Unified Manager e executar as APIs específicas para acessar e gerenciar os clusters do ONTAP sem fornecer credenciais individuais de cluster. O Unified Manager funciona como um ponto único de gerenciamento para executar as APIs nos clusters do ONTAP gerenciados pela sua instância do Unified Manager. A resposta retornada pelas APIs é a mesma que a resposta retornada pelas respectivas APIs REST do ONTAP executadas diretamente do ONTAP.

Após habilitar esse recurso, você poderá 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 o 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 "Primeiros passos com as APIs REST do Active IQ Unified Manager".

Especifique o tempo limite de inatividade no Active IQ Unified Manager

Você pode especificar o valor do tempo limite de inatividade para o Active IQ Unified Manager. Após o tempo de inatividade especificado, o aplicativo faz logout automaticamente. Essa opção está habilitada por padrão.

Você pode desativar este recurso ou modificar o tempo limite em **Geral** > **Configurações de Recursos** > **Tempo Limite de Inatividade**. Após ativar este recurso, você deve especificar o limite de tempo de inatividade (em minutos) no campo **SAIR APÓS**, após o qual o sistema encerra a sessão automaticamente. O valor padrão é 4320 minutos (72 horas).

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

Ative os eventos do portal Active IQ no Active IQ Unified Manager

Você pode especificar se deseja ativar ou desativar os eventos do portal Active IQ. Essa configuração permite que o portal Active IQ descubra e exiba eventos adicionais sobre a configuração do sistema, o cabeamento e assim por diante. Essa opção está ativada por padrão.

Ao ativar esse recurso, o Active IQ Unified Manager exibe os eventos descobertos pelo portal Active IQ. Esses eventos são criados ao executar um conjunto de regras nas mensagens AutoSupport geradas por todos os sistemas de storage monitorados. Esses eventos são diferentes dos outros eventos do Unified Manager e identificam incidentes ou riscos relacionados à configuração do sistema, ao cabeamento, às melhores práticas e aos problemas de disponibilidade.

Você pode optar por ativar ou desativar esse recurso em **Geral** > **Configurações de recursos** > **Active IQ Portal Events**. Em sites sem acesso externo à rede, você deve carregar as regras manualmente em **Gerenciamento de storage** > **Configuração de eventos** > **Carregar regras**.

Este recurso está ativado por padrão. Desativar esse recurso impede que os eventos do Active IQ sejam

descobertos ou exibidos no Unified Manager. Quando estiver desativado, ativar esse recurso permitirá que o Unified Manager receba os eventos do Active IQ em um cluster no horário predefinido de 00:15 para o fuso horário desse cluster.

Ative e desative as configurações de segurança para conformidade no Active IQ Unified Manager

Ao usar o botão **Customize** no painel **Security Dashboard** da página Configurações de recursos, você pode ativar ou desativar os parâmetros de segurança para o monitoramento de conformidade no Unified Manager.

As configurações ativadas ou desativadas nesta página controlam o status geral de conformidade dos clusters e das VMs de storage no Unified Manager. Com base nas seleções, as colunas correspondentes ficam visíveis na visualização **Segurança: todos os clusters** da página de inventário de Clusters e na visualização **Segurança: todas as VMs de storage** da página de inventário de VMs de storage.

Somente usuários com função de administrador podem editar essas configurações.

Os critérios de segurança para seus clusters ONTAP, VMs de storage e volumes são avaliados em relação às recomendações definidas no "Guia de fortalecimento da segurança para o NetApp ONTAP 9". O painel Segurança no dashboard e a página Segurança exibem o status de conformidade de segurança padrão de seus clusters, VMs de storage e volumes. Eventos de segurança também são gerados, e ações de gerenciamento são habilitadas para os clusters e VMs de storage que apresentam violações de segurança.

Personalize as configurações de segurança

Para personalizar as configurações de monitoramento de conformidade de acordo com o seu ambiente ONTAP, siga estas etapas:

Passos

1. Clique em **Geral > Configurações de recursos > Painel de segurança > Personalizar**. A janela pop-up **Personalizar configurações do Painel de segurança** aparece.

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

2. Para ativar ou desativar as configurações personalizadas para seus clusters do 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 ativar ou desativar as configurações personalizadas para suas VMs de storage, selecione a configuração geral necessária em **Storage VM**. Para obter informações sobre as opções para personalizar a conformidade da VM de storage, consulte "Categorias de conformidade de VMs de storage".

Personalize as configurações do AutoSupport e da autenticação

Na seção **AutoSupport Settings**, você pode especificar se o transporte HTTPS deve ser usado para enviar mensagens de AutoSupport do ONTAP.

Na seção **Configurações de Autenticação**, você pode habilitar o Unified Manager para gerar alertas para o

usuário administrador padrão do ONTAP.

Ativar e desativar o upload de scripts no Active IQ Unified Manager

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

Antes de começar

Você precisa ter a função de Application Administrator.

Passos

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

Se você quiser…	Então faça isso…
Desativar scripts	No painel **Script Upload**, mova o botão deslizante para a esquerda.
Ativar scripts	No painel **Script Upload**, mova o botão deslizante para a direita.

Adicione um banner de login no Active IQ Unified Manager

Adicionar um banner de login permite que sua organização exiba informações 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 storage ou administradores, pode visualizar este banner pop-up de login durante o login, logout e o tempo limite da sessão.

Use o console de manutenção

Saiba mais sobre o console de manutenção no Active IQ Unified Manager

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 a ocorrência de problemas.

Dependendo do sistema operacional no qual você instalou o Unified Manager, o console de manutenção oferece 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
- Gere 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 e as configurações do o Unified Manager a partir de uma versão com backup anterior.

Saiba mais sobre o usuário de manutenção no Active IQ Unified Manager

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 Application Administrator na IU da web, e esse usuário 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.

Funcionalidades de diagnóstico do usuário no Active IQ Unified Manager

O objetivo do acesso para diagnóstico é permitir que o suporte técnico ajude 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 orientado pelo suporte técnico, para fins de solução de problemas.

Acesse o console de manutenção no Active IQ Unified Manager

Caso a interface de usuário do Unified Manager não esteja em funcionamento, ou se você precisar executar funções que não estão disponíveis na interface de usuário, você pode acessar o console de manutenção para gerenciar seu sistema Unified Manager.

Antes de começar

Você precisa ter instalado e configurado o Unified Manager.

Após 15 minutos de inatividade, o console de manutenção encerra sua sessão.

Quando instalado no VMware, se você já tiver feito login como usuário de manutenção por meio do console do VMware, não poderá fazer login simultaneamente usando o Secure Shell.

Etapa

1. Siga estes passos 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. Faça 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. Faça login no sistema com o nome e a senha do usuário de manutenção (umadmin). c. Digite o comando `maintenance_console` e pressione Enter.
Windows	a. Faça login no sistema Unified Manager com as credenciais de administrador. b. Inicie o PowerShell como administrador do Windows. c. Digite o comando `maintenance_console` 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 no Active IQ Unified Manager

Se a interface de usuário do Unified Manager não estiver em funcionamento, ou se você precisar executar funções que não estejam disponíveis na interface de usuário, poderá acessar o console de manutenção para reconfigurar seu dispositivo virtual.

Antes de começar

- Você deve ser o usuário de manutenção.
- O appliance virtual deve estar ligado para acessar o console de manutenção.

Passos

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

   Após 15 minutos de inatividade, o console de manutenção encerra sua sessão.

Menus do console de manutenção

Saiba mais sobre os menus do console de manutenção no Active IQ Unified Manager

O console de manutenção consiste em diferentes menus que permitem a você 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 o VMware)
  a. Suporte/Diagnóstico
  b. Redefinir certificado do servidor
  c. Regenerar certificado do cliente
  d. Backup e restauração
  e. Fornecedor de dados externo
  f. Configuração do intervalo de sondagem de desempenho
  g. Desativar autenticação SAML
  h. Visualizar/alterar portas do aplicativo
  i. Configuração do log de depuração
  j. Controlar o acesso à porta 3306 do MySQL
  k. Sair

Você seleciona o número da lista para acessar a opção específica do menu. Por exemplo, para backup e restauração, você seleciona *4*.

Menu de configuração de rede no Active IQ Unified Manager

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 está 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 o endereço IP, a rede, o endereço de broadcast, a máscara de rede, o gateway e os servidores DNS.

- **Alterar configurações de endereço IP**

  Permite que você altere qualquer configuração de rede do appliance virtual, incluindo o endereço IP, a máscara de rede, o gateway ou os servidores DNS. Se você alterar suas configurações de rede de DHCP

para rede estática usando o console de manutenção, não poderá editar o nome do host. Você deve selecionar **Commit Changes** para que as alterações entrem em vigor.

- **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 nomes de domínio**

  Permite alterar os nomes de domínio que você deseja pesquisar ao resolver nomes de host. Você deve selecionar **Confirmar alterações** para que as alterações entrem em vigor.

- **Exibir rotas estáticas**

  Exibe as rotas de rede estáticas atuais.

- **Alterar rotas estáticas**

  Permite adicionar ou excluir rotas de rede estáticas. Você deve selecionar **Commit Changes** para que as alterações entrem em vigor.

  - **Adicionar rota**

    Permite adicionar uma rota estática.

  - **Excluir Rota**

    Permite excluir uma rota estática.

  - **Voltar**

    Retorna ao **Menu Principal**.

  - **Sair**

    Sai do console de manutenção.

- **Desativar interface de rede**

  Desativa todas as interfaces de rede disponíveis. Se houver apenas uma interface de rede disponível, você não poderá desativá-la. Você deve selecionar **Commit Changes** para que as alterações entrem em vigor.

- **Habilitar interface de rede**

  Habilita as interfaces de rede disponíveis. Você deve selecionar **Confirmar alterações** para que as alterações entrem em vigor.

- **Confirmar alterações**

  Aplica quaisquer alterações feitas nas configurações de rede do dispositivo virtual. Você deve selecionar esta opção para que quaisquer alterações feitas entrem em vigor, caso contrário, as alterações não ocorrerão.

- **Enviar ping para um host**

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

- **Restaurar configurações padrão**

  Redefine todas as configurações para o padrão de fábrica. Você deve selecionar **Commit Changes** para que as alterações entrem em vigor.

- **Voltar**

  Retorna ao **Menu Principal**.

- **Sair**

  Sai do console de manutenção.

Utilize o menu Configuração do Sistema no Active IQ Unified Manager

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

Quando o Unified Manager está instalado em um sistema Linux ou Microsoft Windows, somente a opção “Restore from a Unified Manager Backup” 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 funcionando, talvez seja necessário entrar em contato com o suporte técnico.

- **Reiniciar máquina virtual**

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

- **Desligar a máquina virtual**

  Encerra a máquina virtual, interrompendo todos os serviços.

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

- **Alterar <logged in user> senha do usuário**

  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 o da sua localização.

- **Alterar servidor NTP**

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

- **Alterar o serviço NTP**

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

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

  Restaura o banco de dados e as configurações do o Unified Manager a partir 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 appliance virtual está instalado.

- **Voltar**

  Sai do menu Configuração do Sistema e retorna ao menu principal.

- **Sair**

  Sai do menu do console de manutenção.

Utilize o menu Suporte e Diagnóstico no Active IQ Unified Manager

O menu Suporte e Diagnóstico permite gerar um pacote de suporte que você pode enviar ao suporte técnico para obter assistência na resolução de problemas.

As seguintes opções de menu estão disponíveis:

- **Gerar pacote de suporte leve**

  Permite que você crie um pacote de suporte leve que contém apenas 30 dias de logs e registros do banco de dados de configuração, excluindo dados de desempenho, arquivos de gravação de aquisição e heap dump do servidor.

- **Gerar pacote de suporte**

  Permite criar um pacote de suporte completo (arquivo 7-Zip) contendo informações de diagnóstico no diretório base do usuário de diagnóstico. Se o seu sistema estiver conectado à internet, você também pode enviar o pacote de suporte para NetApp.

  O arquivo inclui informações geradas por uma mensagem 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 que normalmente não são incluídos em mensagens AutoSupport nem no pacote de suporte simplificado.

Saiba mais sobre as opções adicionais do menu do console de manutenção no Active IQ Unified Manager

As opções de menu a seguir permitem que você execute diversas tarefas administrativas no servidor 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**.

- **Desativar a autenticação SAML**

  Desativa a autenticação SAML para que o provedor de identidade (IdP) não forneça mais autenticação de logon para os usuários que acessam a GUI do Unified Manager. Essa opção de console normalmente é usada quando um problema com o servidor IdP ou com a configuração SAML impede que os usuários acessem a GUI do Unified Manager.

- **Fornecedor de dados externo**

  Oferece opções para conectar o Unified Manager a um provedor de dados externo. Após estabelecer a conexão, os dados de desempenho são enviados para um servidor externo para que especialistas em desempenho de storage possam gerar gráficos das métricas usando software de terceiro. As seguintes opções são exibidas:

  - **Exibir configuração do servidor**--Exibe as configurações atuais de conexão e de configuração de um provedor de dados externo.
  - **Adicionar / Modificar conexão com o servidor**--Permite inserir novas configurações de conexão para um provedor de dados externo ou alterar as configurações existentes.
  - **Modificar Configuração do Servidor** permite inserir novas configurações para um provedor de dados externo ou alterar as configurações existentes.
  - **Excluir conexão com o servidor**--Exclui a conexão com um provedor de dados externo.

    Após a exclusão da conexão, o Unified Manager perde a conexão com o servidor externo.

- **Backup e Restauração**

  Para obter mais informações, consulte os tópicos em "Gerenciamento de operações de backup e restauração".

- **Configuração do intervalo de sondagem de desempenho**

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

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

- **Visualizar/Alterar portas do aplicativo**

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

- **Controlar 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 meio dessa porta é restrito apenas ao localhost durante uma nova instalação do Unified Manager em sistemas Linux, Windows e VMware vSphere. Esta opção permite alternar a visibilidade dessa porta entre o localhost e hosts remotos, ou seja, se ela estiver habilitada apenas para localhost em seu ambiente, você poderá disponibilizar essa porta também para hosts remotos. Como alternativa, quando ela estiver habilitada para todos os hosts, você poderá restringir o acesso a essa porta apenas ao localhost. Se o acesso tiver sido habilitado anteriormente em hosts remotos, a configuração será mantida em um cenário de upgrade. Você deve verificar as configurações do firewall em sistemas Windows após alternar a visibilidade da porta e desabilitar as configurações do firewall se elas estiverem configuradas para restringir o acesso à porta 3306 do MySQL.

- **Sair**

  Sai do menu do console de manutenção.

Altere a senha do usuário de manutenção no Windows no Active IQ Unified Manager

Você pode alterar a senha do usuário de manutenção do Unified Manager quando necessário.

Passos

1. Na página de login da interface web do Unified Manager, clique em **Esqueci minha senha**.

   Uma página é exibida 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 ao endereço de e-mail definido para esse nome de usuário.

3. Clique no **link de redefinição de senha** no e-mail e defina a nova senha.
4. Retorne à interface web e faça login no Unified Manager usando a nova senha.

Altere a senha umadmin do Active IQ Unified Manager 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 poderá alterar a senha novamente a qualquer momento.

Antes de começar

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

Passos

1. Faça login como usuário raiz no sistema Linux em que o Unified Manager está em execução.
2. Altere a senha do umadmin:

   ```
   passwd umadmin
   ```

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

Altere as portas que o Active IQ Unified Manager utiliza 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 motivos de segurança. As portas padrão são 80 para HTTP e 443 para HTTPS.

Antes de começar

Você precisa ter um ID de usuário e uma senha autorizados para fazer login no console de manutenção do servidor Unified Manager.

> Algumas portas são consideradas inseguras ao usar os navegadores Mozilla Firefox ou Google Chrome. Verifique no seu navegador antes de atribuir um novo número de porta para o tráfego HTTP e HTTPS. Selecionar uma porta insegura pode tornar o sistema inacessível, o que exigiria que você entrasse em contato com o suporte ao cliente para obter uma solução.

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

1. Faça 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 **View/Change Application Ports** e pressione Enter.
3. Caso seja solicitado, digite novamente a senha do usuário de manutenção.
4. Digite os novos números de porta para as portas HTTP e HTTPS, e pressione Enter.

   Deixar o número da porta em branco atribui a porta padrão ao protocolo.

   Será perguntado a você 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 da porta na URL para acessar a interface web do Unified Manager, por exemplo https://host.company.com:1234, https://12.13.14.15:1122, ou https://[2001:db8:0:1]:2123.

Adicionar interfaces de rede ao Active IQ Unified Manager

Você pode adicionar novas interfaces de rede se precisar separar tráfego de rede.

Antes de começar

Você deve ter adicionado a interface de rede ao dispositivo virtual usando o vSphere.

O appliance virtual precisa 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** > **Reiniciar sistema operacional**.

   Após a reinicialização, o console de manutenção poderá 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 ativar a interface de rede.
6. Insira as configurações de rede.

   Você deverá 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 retorna automaticamente ao menu **Configuração de Rede**.

7. Selecione **Confirmar alterações**.

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

Regere o certificado de cliente no Active IQ Unified Manager

Você pode usar o console de manutenção para regenerar o certificado de cliente do Unified Manager. Seu certificado tem um período de validade estendido de cinco anos.

Passos

1. Faça login como usuário de manutenção.
2. Selecione **Regenerar certificado do cliente** e pressione **Enter**.
3. Se o sistema solicitar autenticação, insira as credenciais necessárias.
4. Selecione **Confirm Regeneration** e pressione **Enter**.
5. Após a regeneração do certificado, reinicie o serviço Unified Manager para aplicar as alterações.
6. Para verificar o certificado atualizado, faça login no ONTAP. Visualize o status do certificado do cliente e o status de validade.

Informações relacionadas "Gerencie os certificados do ONTAP com o System Manager"

Adicionar espaço de disco

Adicione espaço de disco ao diretório do banco de dados do Active IQ Unified Manager

O diretório do banco de dados do Unified Manager contém todos os dados de integridade e desempenho coletados dos sistemas ONTAP. Em algumas circunstâncias, pode ser necessário aumentar 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% de ocupação.

As etapas necessárias para adicionar capacidade ao diretório de dados variam dependendo de o Unified Manager estar em execução em um servidor VMware ESXi, em um servidor Red Hat ou em um servidor Microsoft Windows.

Adicione espaço ao diretório de dados em um host Linux no Active IQ Unified Manager

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

Antes de começar

Você deve ter acesso de usuário raiz à máquina Red Hat Enterprise Linux na qual o Unified Manager está instalado.

Recomendamos que você faça backup do banco de dados do Unified Manager antes de aumentar o tamanho do diretório de dados.

Passos

1. Faça login como usuário raiz na máquina Linux na qual você deseja adicionar espaço de disco.
2. Pare o serviço do 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 de disco suficiente para conter os dados no diretório atual `/opt/netapp/data`.
4. Copie o conteúdo e a configuração de privilégios do diretório existente `/opt/netapp/data` para o diretório de dados de backup:

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

5. Se o SE Linux estiver ativado:

   a. Obtenha o tipo do SE Linux para pastas em uma pasta `/opt/netapp/data` existente:

      ```
      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 de 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. Aumente 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` a partir de um disco, não tente montar `/opt/netapp/data` como um compartilhamento NFS ou CIFS. Isso porque, nesse caso, ao tentar expandir o espaço de disco, alguns comandos LVM, como `resize` e `extend`, podem não funcionar como esperado.

8. Confirme se o `/opt/netapp/data` proprietário do diretório (mysql) e o grupo (root) permanecem inalterados:

```
ls -ltr /opt/netapp/ | grep data
```

O sistema retorna uma confirmação semelhante à seguinte:

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. Se o SE Linux estiver ativado, confirme se o contexto do `/opt/netapp/data` 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 desnecessário não cause um erro no banco de dados no futuro.
11. Copie o conteúdo de backup-data de volta para o diretório expandido `/opt/netapp/data`:

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

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

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

13. Inicie o serviço MySQL:

    ```
    systemctl start mysqld
    ```

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

    ```
    systemctl start ocie ocieau
    ```

15. Após todos os serviços serem iniciados, exclua a pasta de backup `/backup-data`:

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

Adicione espaço ao disco de dados em uma máquina virtual no Active IQ Unified Manager

Se você precisar aumentar a quantidade de espaço no disco de dados para o banco de dados do Unified Manager, poderá adicionar capacidade após a instalação aumentando o espaço de disco por meio do console de manutenção do Unified Manager.

Antes de começar

- Você precisa ter acesso ao vSphere Client.
- A máquina virtual não deve ter nenhum snapshot armazenado localmente.
- Você precisa ter as credenciais do usuário de manutenção.

Recomendamos que você faça um 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, em seguida, adicione mais capacidade de disco aos dados `disk 3`. Consulte a documentação da VMware para obter detalhes.

   Em alguns casos raros, a implantação do Unified Manager usa “Hard Disk 2” para o disco de dados em vez de “Hard Disk 3”. Se isso ocorreu na sua implantação, aumente o espaço do disco que for maior. O disco de dados sempre terá mais espaço do que o outro disco.

2. No cliente vSphere, selecione a máquina virtual do Unified Manager e, em seguida, selecione a guia **Console**.
3. Clique na janela do console e, em seguida, faça login no console de manutenção usando seu nome de usuário e senha.
4. No menu principal, digite o número da opção **Configuração do sistema**.
5. No menu de configuração do sistema, insira o número da opção **Aumentar o tamanho do disco de dados**.

Adicionar espaço à unidade lógica em um servidor Windows no Active IQ Unified Manager

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

Manager está instalado.

Antes de começar

Você precisa ter privilégios de administrador do Windows.

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

Passos

1. Faça login como administrador no servidor Windows no qual deseja adicionar espaço de disco.
2. Siga o passo a passo correspondente ao método que deseja usar para adicionar mais espaço:

Opção	Descrição
Em um servidor físico, adicione capacidade à unidade lógica na qual o servidor do Unified Manager está instalado.	Siga os passos descritos no tópico da Microsoft: "Ampliar um Volume Básico"
Em um servidor físico, adicione um disco rígido.	Siga os passos descritos no tópico da Microsoft: "Adicionando discos rígidos"
Em uma máquina virtual, aumente o tamanho de uma partição de disco.	Siga os passos descritos no tópico da VMware: "Aumentar o tamanho de uma partição de disco"

Gerencie o acesso do usuário

Adicionar usuários

Adicionar usuários no Active IQ Unified Manager

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

Antes de começar

- Você precisa ter a função de Application Administrator.
- Para adicionar um usuário ou grupo remoto, você precisa 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 os usuários que acessam a interface gráfica, certifique-se de que esses usuários sejam definidos como usuários “remote”.

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

Se você adicionar um grupo do Active Directory do Windows, todos os membros diretos e subgrupos aninhados poderão se autenticar no Unified Manager, a menos que os subgrupos aninhados estejam

desativados. Se você adicionar um grupo do OpenLDAP ou de outros serviços de autenticação, somente os membros diretos desse grupo poderão se autenticar no Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Usuários**.
2. Na página Users, clique em **Add**.
3. Na caixa de diálogo Add User, selecione o tipo de usuário que você deseja adicionar e insira as informações necessárias.

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

4. Clique em **Add**.

Crie um usuário de banco de dados no Active IQ Unified Manager

Para oferecer suporte a uma conexão entre o Workflow Automation e o Unified Manager, ou para acessar visualizações do banco de dados, você deve primeiro criar um usuário de banco de dados com a função Integration Schema ou Report Schema na interface da web do Unified Manager.

Antes de começar

Você precisa ter a função de Application Administrator.

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 nem ao console de manutenção, e não podem executar chamadas de API.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Usuários**.
2. Na página Users, clique em **Add**.
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 o Workflow Automation	Esquema de integração
Acesso a relatórios e outras visualizações do banco de dados	Esquema do relatório

6. Clique em **Add**.

Editar configurações de usuário no Active IQ Unified Manager

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

de storage a esse usuário.

Antes de começar

Você precisa ter a função de Application Administrator.

Ao modificar a função atribuída a um usuário, as alterações são aplicadas quando ocorre uma das seguintes ações:

- Você faz logout e login novamente no Unified Manager.
- A sessão atingiu o tempo limite de 24 horas.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Usuários**.
2. Na página Users, selecione o usuário para o qual você deseja editar as configurações e clique em **Edit**.
3. Na caixa de diálogo Edit User, edite as configurações apropriadas especificadas para o usuário.
4. Clique em **Salvar**.

Visualizar usuários no Active IQ Unified Manager

Você pode usar a página Usuários para visualizar a lista de usuários que gerenciam objetos de storage 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 a eles.

Antes de começar

Você precisa ter a função de Application Administrator.

Etapa

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

Excluir usuários ou grupos no Active IQ Unified Manager

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 ter reatribuído os eventos atribuídos aos usuários desses grupos.

  Se você excluir usuários locais ou usuários remotos, os eventos atribuídos a esses usuários terão a atribuição removida automaticamente.

- Você precisa ter a função de Application Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Usuários**.
2. Na página Usuários, selecione os usuários ou grupos que deseja excluir e clique em **Excluir**.

3. Clique em **Sim** para confirmar a exclusão.

Saiba mais sobre controle de acesso baseado em funções no Active IQ Unified Manager

O RBAC (controle de acesso baseado em funções) oferece a capacidade de controlar quem tem acesso a vários recursos e funcionalidades no servidor do Active IQ Unified Manager. O 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 você quiser restringir as informações que os administradores podem visualizar e as operações que podem executar, será necessário aplicar funções às contas de administrador que você criar.

O servidor de gerenciamento usa RBAC para login de usuários e permissões de função. Se você não alterou as configurações padrão do servidor de gerenciamento para acesso de usuários administrativos, não precisa fazer login para visualizá-las.

Ao iniciar 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 à conta Application Administrator.

Saiba mais sobre os tipos de usuários no Active IQ Unified Manager

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 Administrator.

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 cria outros usuários 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 de usuário do Unified Manager e executa funções com base na função atribuída pelo usuário de manutenção ou por um usuário com a função Application Administrator.

- **Grupo remoto**

  Um grupo de usuários que acessa a interface do usuário do Unified Manager usando as credenciais armazenadas no servidor de autenticação. O nome dessa conta deve corresponder ao nome de um grupo armazenado no servidor de autenticação. Todos os usuários do grupo remoto recebem acesso à interface do usuário do Unified Manager usando suas credenciais individuais de usuário. Os grupos remotos podem executar funções de acordo com os papéis atribuídos.

- **Usuário remoto**

  Acessa a interface 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 Application Administrator.

- **Usuário do banco de dados**

  Possui acesso somente leitura aos dados no banco de dados do Unified Manager, não tem acesso à interface da web do Unified Manager nem ao console de manutenção e não pode executar chamadas de API.

Saiba mais sobre as funções de usuário no Active IQ Unified Manager

O usuário de manutenção ou o administrador de aplicativos atribui uma função a cada usuário. Cada função contém determinados privilégios. O escopo das atividades que você pode executar no Unified Manager depende da função atribuída e dos privilégios que essa função contém.

O Unified Manager inclui as seguintes funções de usuário predefinidas:

- **Operador**

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

- **Administrador de storage**

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

- **Administrador de aplicativos**

  Configura definições não relacionadas ao gerenciamento de storage. Essa 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 Application Administrator é automaticamente nomeado como “umadmin”.

- **Esquema de Integração**

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

- **Esquema do relatório**

  Esta função permite acesso somente leitura a relatórios e outras visualizações do banco de dados diretamente do banco de dados do Unified Manager. Os bancos de dados que podem ser visualizados incluem:

- netapp_model_view
- netapp_performance
- ocum
- ocum_report
- ocum_report_birt
- opm
- scalemonitor

Saiba mais sobre funções e capacidades de usuário no Active IQ Unified Manager

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

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

Função	Operador	Administrador de storage	Administrador de Aplicativos	Esquema de integração	Esquema do relatório
Visualizar informações do sistema de storage	•	•	•	•	•
Veja outros dados, como históricos e tendências de capacidade	•	•	•	•	•
Visualizar, atribuir e resolver eventos	•	•	•		
Visualize objetos de serviço de storage, como associações de SVM e pools de recursos	•	•	•		
Ver políticas de limite	•	•	•		
Gerenciar objetos de serviço de storage, como associações de SVM e pools de recursos		•	•		
Definir alertas		•	•		

Função	Operador	Administrador de storage	Administrador de Aplicativos	Esquema de integração	Esquema do relatório
Gerencie as opções de gerenciamento de storage		•	•		
Gerenciar políticas de gerenciamento de storage		•	•		
Gerenciar usuários			•		
Gerenciar opções administrativas			•		
Definir políticas de limite			•		
Gerenciar o acesso ao banco de dados			•		
Gerencie a integração com o WFA e forneça acesso às visualizações do banco de dados				•	
Agendar e salvar relatórios		•	•		
Execute operações “Fix It” em Management Actions		•	•		
Fornecer acesso somente leitura às visualizações do banco de dados					•

Gerenciar configurações de autenticação SAML

Ative a autenticação SAML no Active IQ Unified Manager

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

Observe que somente os usuários remotos terão acesso à interface gráfica de usuário do Unified Manager após a autenticação SAML ter sido ativada. Os usuários locais e os usuários de manutenção não poderão acessar a interface. Essa configuração não afeta os usuários que acessam o console de manutenção.

Utilize um provedor de identidade no Active IQ Unified Manager

Ao configurar o Unified Manager para usar um provedor de identidade (IdP) para realizar autenticação SAML para todos os usuários remotos, você precisa estar ciente de algumas configurações obrigatórias para que a conexão com 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 SAML Authentication 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 Avançado (AES): AES-128 e AES-256
- Algoritmo de Hash Seguro (SHA): SHA-1 e SHA-256

Provedores de identidade validados

- O Shibboleth
- O Active Directory Federation Services (ADFS)

Requisitos de configuração do ADFS

- Você deve definir três regras de declaração 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
SAM-account-name	ID do nome
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Grupos de tokens — nome não qualificado	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Você deve definir o método de autenticação como “Forms Authentication” ou os usuários poderão receber um erro ao sair do Unified Manager . Siga estas etapas:
  a. Abra o ADFS Management Console.
  b. Clique na pasta Políticas de Autenticação na exibição 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 “Forms Authentication” em vez do padrão “Windows Authentication”.
- Em alguns casos, o login pelo IdP é rejeitado quando o certificado de segurança do Unified Manager é assinado por uma CA. Existem duas soluções alternativas para resolver esse problema:
  - Siga as instruções indicadas no link para desativar a verificação de revogação no servidor ADFS da parte confiável associada ao certificado de AC encadeada:

    "Desativar a verificação de revogação por confiança de 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 está configurado para 5 minutos, portanto a diferença de horário entre o servidor IdP e o servidor Unified Manager não pode ser superior a 5 minutos, caso contrário, a autenticação falhará.

Ative a autenticação SAML no Active IQ Unified Manager

Você pode habilitar a autenticação Security Assertion Markup Language (SAML) para que os usuários remotos sejam autenticados por um provedor de identidade (IdP) seguro antes de acessarem a interface de usuário 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 compatível com o Unified Manager e deve estar configurado.
- Você precisa ter a URL do IdP e os metadados.
- Você precisa ter acesso ao servidor IdP.

Após habilitar a autenticação SAML no Unified Manager, os usuários não poderão acessar a interface gráfica de usuário até que o IdP seja configurado com as informações de 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 de configurar o Unified Manager.

Somente usuários remotos terão acesso à interface gráfica de usuário do Unified Manager após a autenticação SAML ser ativada. Usuários locais e usuários de manutenção não poderão acessar a interface do usuário. Essa configuração não afeta usuários que acessam o console de manutenção, os comandos do Unified Manager ou as ZAPIs.

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

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação SAML**.
2. Selecione a caixa de seleção **Enable SAML authentication**.

   São exibidos os campos necessários para configurar a conexão IdP.

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

   Se o servidor IdP estiver acessível diretamente a partir do servidor do Unified Manager, você pode clicar no botão **Obter metadados do IdP** após inserir o URI do IdP para preencher automaticamente o campo de metadados do IdP.

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 agora.

5. Clique em **Salvar**.

   Uma caixa de mensagem será 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.

Caso ainda não tenha feito isso, acesse seu IdP e insira a 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**.

Altere o provedor de identidade de autenticação SAML no Active IQ Unified Manager

Você pode alterar o provedor de identidade (IdP) que o Unified Manager usa para autenticar usuários remotos.

Antes de começar

- Você precisa ter a URL do IdP e os metadados.
- Você precisa ter acesso ao IdP.

O novo IdP pode ser configurado antes ou depois de configurar o 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 **Fetch IdP Metadata** após inserir a URL do IdP para preencher automaticamente o campo IdP Metadata.

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 a URI do servidor do Unified Manager e os metadados para concluir a configuração.

Na próxima vez que usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles deverão inserir suas credenciais na nova página de login do IdP em vez da antiga página de login do IdP.

Atualize as configurações de autenticação SAML após uma alteração no certificado de segurança do Active IQ 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 é atualizado se você renomear o sistema host, atribuir um novo endereço IP ao sistema host ou alterar manualmente o certificado de segurança do sistema.

Após a alteração do certificado de segurança e a reinicialização do servidor do Unified Manager, a autenticação SAML deixará de funcionar, e os usuários não poderão acessar a interface gráfica do Unified Manager. Você deve atualizar as configurações de autenticação SAML tanto no servidor IdP quanto no servidor do Unified Manager para reativar o acesso à interface de usuário.

Passos

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

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

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

Provedor de identidade	Etapas de configuração
ADFS	a. Exclua a entrada de confiança da parte confiável existente na interface gráfica de gerenciamento do ADFS. b. Adicione uma nova entrada de confiança de terceira parte confiável usando o `saml_sp_metadata.xml`do servidor Unified Manager atualizado. c. Defina as três regras de declaração 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.

Provedor de identidade	Etapas de configuração
O Shibboleth	a. Atualize o novo FQDN do servidor do Unified Manager nos arquivos `attribute-filter.xml` e `relying-party.xml`. b. Reinicie o servidor web Apache Tomcat e aguarde até que a porta 8005 fique online.

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

Desative a autenticação SAML no Active IQ Unified Manager

Você pode desativar a autenticação SAML quando desejar interromper a autenticação de usuários remotos por meio de um provedor de identidade (IdP) seguro antes que eles possam fazer login na interface web do Unified Manager. Quando a autenticação SAML está desativada, os provedores de serviço de diretório configurados, como o Active Directory ou o LDAP, realizam a autenticação de login.

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

Você também pode desativar a autenticação SAML usando o console de manutenção do Unified Manager, caso não tenha acesso à interface gráfica de usuário.

O Unified Manager é reiniciado automaticamente após a desativação da autenticação SAML.

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 será 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 os usuários remotos tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do Unified Manager em vez da página de login do IdP.

Acesse seu IdP e exclua o URI do servidor do Unified Manager e os metadados.

Desative a autenticação SAML no console de manutenção do Active IQ Unified Manager

Pode ser necessário desativar a autenticação SAML no console de manutenção quando não houver acesso à interface gráfica do Unified Manager. Isso pode ocorrer em casos de configuração incorreta ou se o IdP estiver inacessível.

Antes de começar

Você precisa ter acesso ao console de manutenção como o usuário de manutenção.

Quando a autenticação SAML está desativada, os provedores de serviço de diretório configurados, como Active Directory ou LDAP, realizam a autenticação de login. Os usuários locais e os usuários de manutenção poderão acessar a interface gráfica do usuário, além dos usuários remotos configurados.

Você também pode desativar a autenticação SAML na página Setup/Authentication da interface de usuário.

O Unified Manager é reiniciado automaticamente após a desativação da autenticação SAML.

Passos

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

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

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

Na próxima vez que os usuários remotos tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do Unified Manager em vez da página de login do IdP.

Caso necessário, acesse seu IdP e exclua a URL do servidor do Unified Manager e os metadados.

Utilize a página de autenticação SAML no Active IQ Unified Manager

Você pode usar a página de autenticação SAML para configurar o Unified Manager para autenticar usuários remotos usando SAML por meio de um provedor de identidade (IdP) seguro antes que eles possam fazer login na interface web do Unified Manager.

- Você precisa ter a função Application Administrator para criar ou modificar a configuração do SAML.
- Você precisa ter configurado a autenticação remota.
- Você deve ter configurado pelo menos um usuário remoto ou um grupo remoto.

Após configurar a autenticação remota e os usuários remotos, você pode selecionar a caixa de seleção "Ativar autenticação SAML" para habilitar a autenticação usando um provedor de identidade seguro.

- **URI do IdP**

  O URI para acessar o IdP a partir do servidor Unified Manager. Veja abaixo alguns exemplos de URIs.

  Exemplo de URI do ADFS:

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

  Exemplo de URI do Shibboleth:

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

- **Metadados do IdP**

Os metadados do IdP em formato XML.

Se o URL do IdP estiver acessível a partir do servidor do Unified Manager, você pode 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**

  Os metadados do sistema host em formato XML.

Gerenciar autenticação

Editar servidores de autenticação no Active IQ Unified Manager

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

Antes de começar

Você precisa ter a função de Application Administrator.

Passos

1. No painel de navegação à esquerda, 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 no Active IQ Unified Manager

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

Antes de começar

Você precisa ter a função de Application Administrator.

Ao excluir um servidor de autenticação, os usuários ou grupos remotos desse servidor de autenticação não poderão mais acessar o Unified Manager.

Passos

1. No painel de navegação à esquerda, 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 ativada, os certificados associados ao servidor de autenticação serão excluídos juntamente com o servidor de autenticação.

Autentique com o Active Directory ou OpenLDAP no Active IQ Unified Manager

Você pode habilitar a autenticação remota no servidor de gerenciamento e configurar o servidor de gerenciamento para se comunicar com seus servidores de autenticação, para que os usuários desses 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:

- O Microsoft Active Directory

  Você não pode usar o Microsoft Lightweight Directory Services.

- O OpenLDAP

Você pode selecionar o serviço de autenticação necessário e adicionar os servidores de autenticação apropriados para permitir que os usuários remotos no servidor de autenticação acessem o Unified Manager. As credenciais de usuários ou grupos remotos são mantidas pelo servidor de autenticação. O servidor de gerenciamento usa o Protocolo Lightweight Directory Access Protocol (LDAP) para autenticar usuários remotos no servidor de autenticação configurado.

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

Registro de auditoria

Saiba mais sobre os registros de auditoria no Active IQ Unified Manager

É possível detectar se os logs de auditoria foram comprometidos usando os 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 de usuário e das APIs expostas publicamente do Active IQ Unified Manager.

Você pode usar a **Visualização de arquivos: log de auditoria** para visualizar e acessar todos os arquivos de log de auditoria disponíveis no seu Active IQ Unified Manager. Os arquivos na Visualização de arquivos: log de auditoria são listados com base na data de criação. Essa visualização exibe informações de todos os logs de auditoria capturados desde a instalação ou atualização até o momento 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 inativo, compactado e armazenado no sistema.
ADULTERADO	Arquivo comprometido por um usuário que editou o arquivo manualmente.
EXCLUSÃO MANUAL	Arquivo que foi excluído por um usuário autorizado.
ROLLOVER_DELETE	Arquivo excluído devido à remoção com base na Política de Configuração de Rotação.
UNEXPECTED_DELETE	Arquivo que foi excluído por motivos desconhecidos.

A página de log de auditoria inclui os seguintes botões de comando:

- Configurar
- Excluir
- Download

O botão **EXCLUIR** permite excluir qualquer um dos logs de auditoria listados na visualização Logs de auditoria. Você pode excluir um log de auditoria e, opcionalmente, fornecer um motivo para excluir o arquivo, o que ajuda no futuro a determinar se a exclusão foi válida. A coluna MOTIVO lista o motivo juntamente com o nome do usuário que realizou a operação de exclusão.

Excluir um arquivo de log remove o arquivo do sistema, mas não exclui a entrada na tabela do DB.

Você pode baixar os logs de auditoria do Active IQ Unified Manager usando o botão **DOWNLOAD** na seção Audit Logs e exportar os arquivos de log de auditoria. Os arquivos marcados como “NORMAL” ou “TAMPERED” são baixados em formato `.gzip` compactado.

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 completo do AutoSupport é gerado, o pacote de suporte inclui arquivos de log de auditoria ativos e arquivados. Mas, quando um pacote de suporte simplificado é gerado, ele inclui apenas os logs de auditoria ativos. Os logs de auditoria arquivados não são incluídos.

Configurar os registros de auditoria do Active IQ Unified Manager

Você pode usar o botão **Configure** na seção Logs de Auditoria para configurar a política de rotação dos arquivos de log de auditoria e também habilitar o registro remoto dos Logs de Auditoria.

Você pode definir os valores em **MAX FILE SIZE** e **AUDIT LOG RETENTION DAYS** de acordo com a quantidade e a frequência de dados que deseja armazenar no sistema. O valor no campo **TOTAL AUDIT LOG SIZE** é o tamanho total dos dados do log de auditoria presentes no sistema. A política de rollover é determinada pelos valores no campo **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** e **TOTAL AUDIT LOG SIZE**. Quando o tamanho do backup do log de auditoria atinge o valor configurado em **TOTAL AUDIT LOG**

SIZE, 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 de **AUDIT LOG RETENTION DAYS** corresponde ao número de dias durante os quais os arquivos de log de auditoria são preservados. Qualquer arquivo mais antigo que o valor definido neste campo passa por rollover.

Passos

1. Clique em **Logs 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**.

   Para ativar o registro remoto, selecione **Ativar registro remoto**.

Ative o registro remoto de logs de auditoria no Active IQ Unified Manager

Você pode selecionar a caixa de seleção **Habilitar registro remoto** na caixa de diálogo Configurar logs de auditoria para habilitar o registro remoto de auditoria. Você pode usar esse recurso para transferir logs de auditoria para um servidor Syslog remoto. Isso permitirá que você gerencie seus logs de auditoria quando houver restrições de espaço.

O registro remoto dos logs de auditoria fornece um backup à prova de adulteração 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**, selecione a caixa de seleção **Habilitar registro remoto**.

   São exibidos campos adicionais para configurar o registro remoto.

2. Digite o **HOSTNAME** e a **PORT** do servidor remoto ao qual você deseja se conectar.
3. No campo **CERTIFICADO DA CA DO SERVIDOR**, clique em **PROCURAR** para selecionar um certificado público do servidor de destino.

   O certificado deve ser carregado no formato `.pem`. Este certificado deve ser obtido do servidor Syslog de destino e não deve estar expirado. O certificado deve conter o “hostname” selecionado como parte do atributo `SubjectAltName`(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. Selecione a caixa de seleção **Habilitar autenticação de cliente** se o servidor Syslog de destino exigir autenticação baseada em certificado.

   Você precisará baixar o certificado de autenticação de cliente e carregá-lo no servidor Syslog antes de salvar a configuração do Log de Auditoria, caso contrário, a conexão falhará. Dependendo do tipo de servidor Syslog, talvez seja necessário criar um hash do certificado de autenticação de cliente.

   Exemplo: o syslog-ng requer que uma <hash> do certificado seja criada usando o comando `openssl x509 -noout -hash -in cert.pem`, e então você deve criar simbolicamente um link do certificado de autenticação de cliente para um arquivo nomeado com <hash> .0.

7. Clique em **Salvar** para configurar a conexão com o seu servidor e ativar o registro remoto.

   Você será redirecionado para a página de Registros de Auditoria.

   O valor de **Tempo limite de conexão** pode afetar a configuração. Se a configuração demorar mais para responder do que o valor definido, isso pode levar a uma falha na configuração devido a um erro de conexão. Para estabelecer uma conexão bem-sucedida, aumente o valor de **Tempo limite de conexão** e tente a configuração novamente.

Utilize a página de autenticação remota no Active IQ Unified Manager

Você pode usar a página de autenticação remota para configurar o Unified Manager para se comunicar com seu servidor de autenticação e autenticar usuários remotos que tentam fazer login na interface web do Unified Manager.

Você precisa ter a função de Application Administrator ou Storage Administrator.

Depois que você selecionar a caixa de seleção Ativar autenticação remota, poderá 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 o Active Directory, o OpenLDAP, ou para especificar seu próprio mecanismo de autenticação. Você só pode especificar um serviço de autenticação se tiver habilitado a autenticação remota.

  - **Active Directory**
    - Nome do administrador

      Especifica o nome 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 diferenciado base será **cn=ou,dc=domain,dc=com**.

    - Desativar pesquisa de grupo aninhado

      Especifica se a opção de pesquisa de grupos aninhados deve ser ativada ou desativada. Por padrão, essa opção está desativada. Se você usa o Active Directory, pode acelerar a autenticação desativando o suporte a grupos aninhados.

    - Usar conexão segura

      Especifica o serviço de autenticação usado para se comunicar com servidores de autenticação.

  - **O OpenLDAP**

- Nome diferenciado de bind

  Especifica o nome diferenciado de bind que é usado juntamente com o nome diferenciado base para encontrar usuários remotos no servidor de autenticação.

- Senha de bind

  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 diferenciado base será **cn=ou,dc=domain,dc=com**.

- Usar conexão segura

  Especifica que o LDAP seguro é usado para se comunicar com servidores de autenticação LDAP.

◦ **Outros**

- Nome diferenciado de bind

  Especifica o nome diferenciado de vinculação que é usado juntamente com o nome diferenciado base para encontrar usuários remotos no servidor de autenticação que você configurou.

- Senha de bind

  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 diferenciado 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 os nomes de login dos usuários a serem autenticados pelo servidor de gerenciamento.

- Atributo de associação a grupo

  Especifica um valor que atribui a associação ao grupo de servidores de gerenciamento a usuários remotos com base em um atributo e valor especificados no servidor de autenticação do usuário.

- UGID

  Se os usuários remotos estiverem incluídos como membros de um objeto GroupOfUniqueNames no servidor de autenticação, esta opção permite atribuir aos usuários remotos a associação ao

grupo do servidor de gerenciamento com base em um atributo especificado nesse objeto GroupOfUniqueNames.

- Desativar pesquisa de grupo aninhado

  Especifica se a opção de pesquisa de grupos aninhados deve ser ativada ou desativada. Por padrão, essa opção está desativada. Se você usa o Active Directory, pode acelerar a autenticação desativando o suporte a grupos aninhados.

- Membro

  Especifica o nome do atributo que o 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 remoto.

> Os valores que você inserir para os atributos *Member*, *User Object Class* e *Group Object Class* devem ser os mesmos adicionados nas configurações do Active Directory, do OpenLDAP e do LDAP. Caso contrário, a autenticação poderá falhar.

- Usar conexão segura

  Especifica o serviço de autenticação usado para se comunicar 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 de usuários ou grupos remotos são mantidas pelo servidor de autenticação.

- **Botões de comando**

  Permite adicionar, editar ou excluir servidores de autenticação.

  - Adicionar

    Permite adicionar um servidor de autenticação.

  Se o servidor de autenticação que você está adicionando fizer parte de um par de alta disponibilidade (usando o mesmo banco de dados), você também poderá adicionar o servidor de autenticação 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 ao autenticar um usuário ou grupo remoto.

  Durante os testes, se você especificar apenas o nome de usuário, o servidor de gerenciamento procurará o usuário remoto no servidor de autenticação, mas não o autenticará. Se você especificar o nome de usuário e a senha, o servidor de gerenciamento procurará e autenticará o usuário remoto.

  Não é possível testar a autenticação se a autenticação remota estiver desativada.

Gerenciar certificados de segurança

Visualize o certificado de segurança HTTPS no Active IQ Unified Manager

Você pode comparar os detalhes do certificado HTTPS com o certificado obtido no seu navegador para garantir que a conexão criptografada do seu navegador com o Unified Manager não esteja sendo interceptada.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

A visualização do certificado permite verificar o conteúdo de um certificado regenerado ou visualizar os Nomes alternativos 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 na parte superior da página

Caso você precise visualizar informações mais detalhadas sobre o certificado de segurança do que as exibidas na página HTTPS Certificate, você pode visualizar o certificado de conexão no seu navegador.

Faça o download de uma solicitação de assinatura de certificado HTTPS no Active IQ Unified Manager

Você pode baixar uma solicitação de assinatura de certificado para o certificado de segurança HTTPS atual para que você possa fornecer o arquivo a uma Autoridade Certificadora (AC) para assiná-lo. Um certificado assinado por uma AC ajuda a evitar

ataques do tipo "man-in-the-middle" e oferece melhor proteção de segurança do que um certificado autoassinado.

Antes de começar

Você precisa ter a função de Application Administrator.

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 a uma autoridade de certificação para que ela o assine e, em seguida, instale o certificado assinado.

Instale um certificado HTTPS assinado por uma Autoridade Certificadora (CA) no Active IQ Unified Manager

Você pode fazer upload e instalar um certificado de segurança depois que uma Autoridade Certificadora (AC) o assinar e devolver. O arquivo que você faz upload e instala deve ser uma versão assinada do certificado autoassinado existente. Um certificado assinado por uma AC ajuda a evitar ataques "man-in-the-middle" e oferece 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 enviou para assinatura por uma autoridade certificadora
- Salvou a cadeia de certificados no formato PEM
- Inclui todos os certificados na cadeia, do certificado do servidor do Unified Manager até o certificado raiz de assinatura, incluindo quaisquer certificados intermediários presentes

Você precisa ter a função de Application Administrator.

Se a validade do certificado para o qual um CSR foi criado for superior a 397 dias, a CA reduzirá essa validade para 397 dias 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 que aparece, clique em **Escolher arquivo…** para localizar o arquivo que deseja carregar.
4. Selecione o arquivo e clique em **Instalar** para instalar o arquivo.

   Para informações, consulte "Instalando um certificado HTTPS gerado com 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-----
```

Saiba mais sobre certificados HTTPS gerados usando ferramentas externas no Active IQ Unified Manager Unified Manager

Você pode instalar certificados autoassinados ou assinados por uma Autoridade Certificadora (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 um par de chaves pública-privada gerado externamente. Os algoritmos de par de chaves permitidos são “RSA” e “EC”. A opção **Install HTTPS Certificate** está disponível na página HTTPS Certificates, na seção General. 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. Certificados das ACs em ordem inversa até a raiz, que são usados para assinar o certificado acima

Formato para carregar um certificado com um par de chaves EC

As curvas permitidas são “prime256v1” e “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 deverá reiniciar a instância do Active IQ Unified Manager para que as alterações entrem em vigor.

Verificações ao carregar certificados gerados externamente

O sistema realiza verificações durante o upload de um certificado gerado usando ferramentas externas. Se alguma das verificações falhar, o certificado será rejeitado. Há também validações incluídas para os certificados gerados a partir da CSR no produto e para os certificados gerados usando ferramentas externas.

- A chave privada informada é validada em relação ao certificado do host informado.
- O Common Name (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 estar no futuro, e a data de expiração da validade do certificado não deve estar no passado.

- Se existir CA intermediária ou CA, a data de início da validade do certificado não deve estar no futuro e a data de expiração da validade não deve estar no passado.

A chave privada na entrada não deve estar criptografada. Se houver chaves privadas criptografadas, elas serão rejeitadas pelo sistema.

Exemplo 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Exemplo 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Exemplo 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Se a instalação do certificado falhar, consulte o artigo da base de conhecimento (KB): "O ActiveIQ Unified Manager falha ao instalar um certificado gerado externamente"

Descrições de páginas para gerenciamento de certificados

Saiba mais sobre a página de certificado HTTPS em o Active IQ Unified Manager

A página de Certificado HTTPS permite visualizar o certificado de segurança atual, baixar uma solicitação de assinatura de certificado, gerar um novo certificado HTTPS autoassinado ou instalar um novo certificado HTTPS.

Se você não gerou um novo certificado HTTPS autoassinado, o certificado exibido nesta página é o certificado gerado durante a instalação.

Botões de comando

Os botões de comando permitem realizar as seguintes operações:

- **Baixar solicitação de assinatura de certificado HTTPS**

Faz o download de uma solicitação de certificação para o certificado HTTPS atualmente instalado. Seu navegador solicitará que você salve o arquivo <hostname>.csr para que você possa fornecê-lo a uma Autoridade Certificadora para assinatura.

- **Instalar certificado HTTPS**

  Permite fazer upload e instalar um certificado de segurança após uma Autoridade de Certificação tê-lo assinado e devolvido. O novo certificado entra em vigor após você reiniciar o servidor de gerenciamento.

- **Regenerar certificado HTTPS**

  Permite gerar um novo certificado HTTPS autoassinado, que substitui o certificado de segurança atual. O novo certificado entra em vigor após reiniciar o Unified Manager.

Regenerar a caixa de diálogo de certificado HTTPS em Active IQ Unified Manager

A caixa de diálogo "Regenerar certificado HTTPS" permite personalizar as informações de segurança e, em seguida, gerar um novo certificado HTTPS com essas informações.

As informações atuais do certificado aparecem nesta página.

As opções “Regenerar usando os atributos atuais do certificado” e “Atualizar os atributos atuais do certificado” permitem regenerar o certificado com as informações atuais ou gerar 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 contato com sua organização; normalmente, o endereço de e-mail do administrador de certificados ou do departamento de TI.

- **Empresa**

  Opcional. Normalmente, o nome registrado da sua empresa.

- **Departamento**

  Opcional. O nome do departamento em sua empresa.

- **Cidade**

  Opcional. A cidade onde sua empresa está localizada.

- **Estado**

  Opcional. O estado ou província onde sua empresa está localizada, sem abreviação.

- **País**

  Opcional. O país onde sua empresa está localizada. Normalmente, trata-se de um código ISO de duas letras do país.

- **Nomes Alternativos**

  Obrigatório. Nomes de domínio adicionais, não primários, que podem ser usados para acessar este servidor além do localhost existente ou de outros endereços de rede. Separe cada nome alternativo com uma vírgula.

  Selecione a caixa de seleção “Excluir informações de identificação local (por exemplo, localhost)” se você 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 você deixar o campo em branco, o certificado resultante não terá um campo Nomes Alternativos.

- **TAMANHO DA CHAVE (ALGORITMO DA CHAVE: RSA)**

  O algoritmo de chave está definido como RSA. Você pode selecionar um dos tamanhos de chave: 2048, 3072 ou 4096 bits. O tamanho de chave padrão é 2048 bits.

- **PERÍODO DE VALIDADE**

  O período de validade padrão é de 397 dias. Se você atualizou de uma versão anterior, poderá ver que a validade do certificado anterior permaneceu inalterada.

Para obter mais informações, consulte "Gerando certificados HTTPS".

Monitorar e gerenciar o armazenamento

Introdução ao Active IQ Unified Manager

Saiba mais sobre o Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente OnCommand Unified Manager) permite monitorar e gerenciar a integridade e o desempenho de seus sistemas de storage ONTAP a partir de uma única interface.

O Unified Manager oferece os seguintes recursos:

- Descoberta, monitoramento e notificações para sistemas com o software ONTAP instalado.
- Painel para mostrar a integridade da capacidade, da segurança e do desempenho do ambiente.
- Infraestrutura aprimorada para alertas, eventos e limiares.
- Exibe gráficos detalhados que representam 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 proporção de cache.
- Identifica cargas de trabalho que estão sobrecarregando 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 solucionar determinados incidentes e eventos, além de um botão "Fix It" para alguns eventos, permitindo que você resolva o problema imediatamente.
- Integra-se com o 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.

Saiba mais sobre monitoramento de saúde no Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente o 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 de servidor do Unified Manager oferece escalabilidade, suporte e recursos aprimorados de monitoramento e notificação.

As principais funcionalidades do Unified Manager incluem monitoramento, emissão de alertas, gerenciamento da disponibilidade e da capacidade dos clusters, gerenciamento de recursos de proteção e agrupamento de dados de diagnóstico e envio deles ao 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 executar para solucionar os problemas. Você pode configurar alertas para eventos para que, quando ocorrerem problemas, você receba notificações 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 a essas anotações por meio de regras.

Você também pode planejar os requisitos de armazenamento dos objetos do seu cluster usando as informações fornecidas nos gráficos de capacidade e saúde do respectivo objeto de cluster.

Capacidade física e lógica

O Unified Manager utiliza os conceitos de espaço físico e lógico usados para objetos de storage do ONTAP.

- Capacidade física: o espaço físico refere-se aos blocos físicos de armazenamento utilizados no volume. A "capacidade física utilizada" é normalmente menor que a capacidade lógica utilizada devido à redução de dados dos recursos de eficiência de storage, como deduplicação e compressão.
- Capacidade lógica: o espaço lógico refere-se ao espaço utilizável (os blocos lógicos) em um volume. O espaço lógico refere-se a como o espaço teórico pode ser usado, sem considerar os resultados da deduplicação ou da compressão. O "espaço lógico usado" é o espaço físico usado mais a economia gerada pelos recursos de eficiência de storage, como deduplicação e compressão, que foram configurados. Essa medição geralmente parece maior do que a capacidade física usada porque não reflete a compressão de dados e outras reduções no espaço físico. Assim, a capacidade lógica total pode ser maior do que o espaço provisionado.

Unidades de medida de capacidade

O Unified Manager calcula a capacidade de storage 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, elas são exibidas no Unified Manager como KiB, MiB, GiB, TiB e PiB.

As unidades usadas para a taxa de transferência continuam sendo kilobytes por segundo (Kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) ou terabytes por segundo (Tbps) e assim por diante, para todas as versões do ONTAP.

Unidade de capacidade exibida no 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
TB	TiB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 bytes

Saiba mais sobre monitoramento de desempenho no Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente OnCommand Unified Manager) oferece recursos de monitoramento de desempenho e análise da causa raiz de eventos para sistemas que executam o software NetApp ONTAP.

O Unified Manager ajuda você a identificar cargas de trabalho que estão sobrecarregando 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 ultrapassado. 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 volumes FlexGroup que você criou em seu cluster.

- Cargas de trabalho definidas pelo sistema

  Essas cargas de trabalho consistem em atividades internas do sistema.

Use as APIs REST do Active IQ Unified Manager

O Active IQ Unified Manager fornece APIs REST para você visualizar informações sobre o monitoramento e o gerenciamento do seu ambiente de storage. As APIs também permitem o provisionamento e o gerenciamento de objetos de storage com base em políticas.

Você também pode executar APIs do ONTAP em todos os clusters gerenciados pelo ONTAP usando o gateway de API compatível com o Unified Manager.

Para obter informações sobre as REST APIs do Unified Manager, consulte "Primeiros passos com as APIs REST do Active IQ Unified Manager".

O que o servidor Unified Manager faz

Saiba mais sobre o servidor Active IQ Unified Manager

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

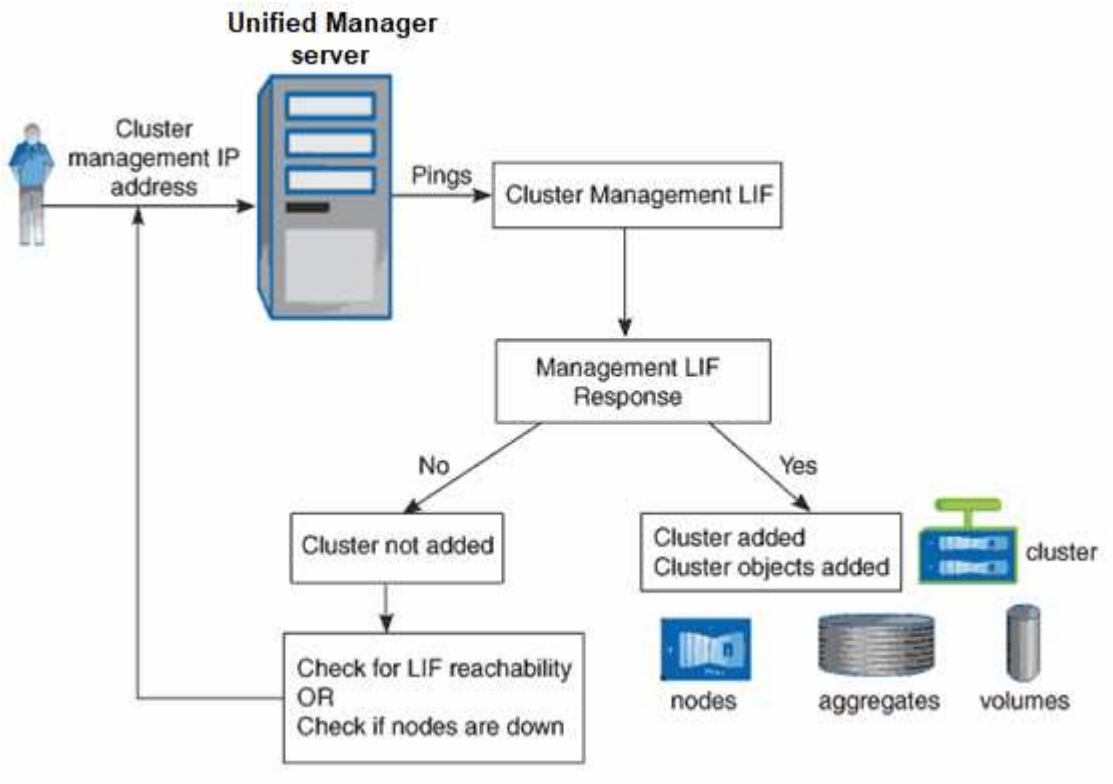
O Unified Manager coleta informações do cluster, armazena os dados no banco de dados e os analisa para verificar se há algum problema no cluster.

Aprenda como funciona o processo de descoberta de clusters no Active IQ Unified Manager

Depois de adicionar o cluster ao Unified Manager, o servidor descobre os objetos do cluster e os adiciona ao seu banco de dados. Compreender como o processo de descoberta funciona ajuda você a gerenciar os clusters da sua organização e seus respectivos objetos.

O intervalo de monitoramento padrão é de 15 minutos: se você adicionou um cluster ao servidor do Unified Manager, leva 15 minutos para exibir os detalhes do cluster na UI do Unified Manager.

A imagem a seguir ilustra o processo de descoberta no Active IQ Unified Manager:



Entenda a interface de usuário

Saiba mais sobre a interface de usuário do Active IQ Unified Manager

A interface de usuário do Unified Manager consiste principalmente em um painel que fornece uma visão geral dos objetos que são monitorados. A interface de usuário também permite visualizar todos os objetos do cluster.

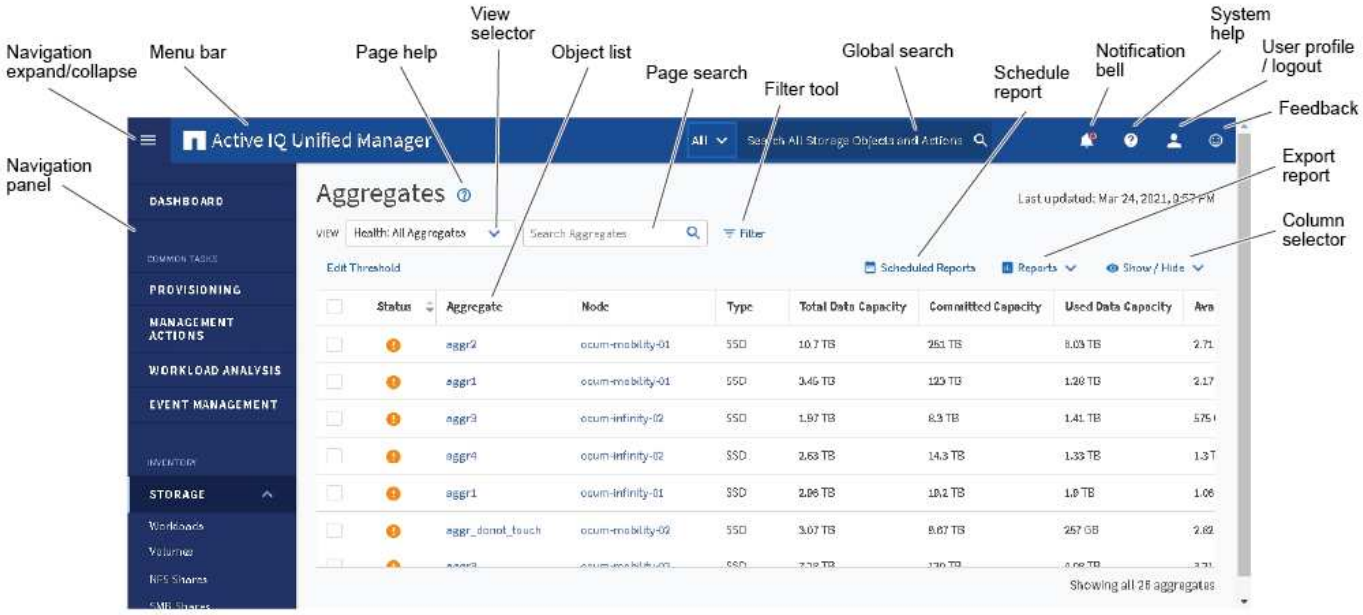
Você pode selecionar uma visualização preferida e usar os botões de ação conforme necessário. Sua configuração de tela é salva em um espaço de trabalho, de modo que todas as funcionalidades necessárias estejam disponíveis ao iniciar o Unified Manager. No entanto, ao navegar de uma visualização para outra e, em seguida, retornar, a visualização pode não ser a mesma.

Layouts de janela típicos no Active IQ Unified Manager

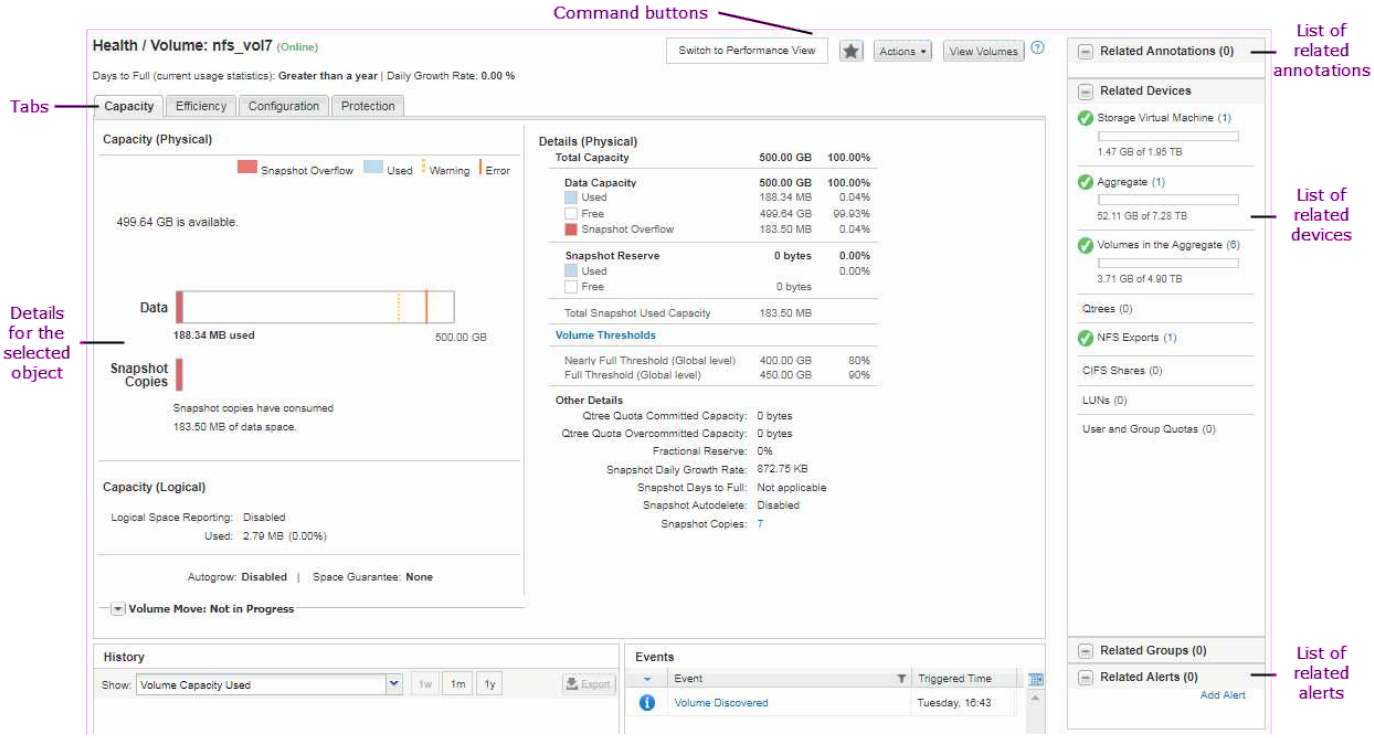
Compreender os layouts típicos das janelas ajuda você a navegar e usar o Active IQ Unified Manager com eficiência. A maioria das janelas do Unified Manager é semelhante a um de dois layouts gerais: lista de objetos ou detalhes. A configuração de exibição recomendada é de pelo menos 1280 por 1024 pixels.

Nem todas as janelas contêm todos os elementos nos diagramas a seguir.

Layout da janela da lista de objetos



Layout da janela de detalhes do objeto



Personalizando o layout da janela no Active IQ Unified Manager

O Active IQ Unified Manager permite personalizar o layout das informações nas páginas de objetos de armazenamento e rede. Ao personalizar as janelas, você pode controlar quais dados são visíveis e como eles são exibidos.

- **Ordenação**

  Você pode clicar no cabeçalho da coluna para alterar a ordem de classificação das entradas da coluna. Ao

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 e personalizar a exibição de informações nas páginas de objetos de armazenamento e rede, de forma que apenas as entradas que correspondam às condições fornecidas sejam exibidas. Você aplica os filtros no painel Filtros.

  O painel Filtros permite filtrar a maioria das colunas com base nas opções selecionadas. Por exemplo, na visualização 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 os dados de capacidade nas unidades apropriadas, arredondados para duas casas decimais. Isso também se aplica ao filtrar colunas de capacidade. Por exemplo, se você usar o filtro na coluna Total Data Capacity na visualização Health: All Aggregates para filtrar dados maiores que 20.45 GB, a capacidade real de 20.454 GB é exibida como 20.45 GB. Da mesma forma, se você filtrar dados menores que 20.45 GB, a capacidade real de 20.449 GB é exibida como 20.45 GB.

  Se você usar o filtro na coluna "Available Data %" na visualização "Health: All Aggregates" 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%.

- **Ocultar ou exibir as colunas**

  Você pode clicar no ícone de exibição de colunas (**Mostrar/Ocultar**) para selecionar quais colunas deseja exibir. Depois de selecionar as colunas desejadas, você pode reordená-las arrastando-as com o mouse.

- **Buscando**

  Você pode usar a caixa de pesquisa para buscar determinados atributos de objetos e ajudar a refinar a lista de itens na página de inventário. Por exemplo, você pode digitar "cloud" para refinar a lista de volumes na página de inventário de volumes e ver todos os volumes que contêm a palavra "cloud".

- **Exportando dados**

  Você pode clicar no botão **Reports** (ou no botão **Export** para exportar dados para um arquivo `(.csv)` de valores separados por vírgulas, `(.pdf)` documento ou arquivo do Microsoft Excel `(.xlsx)` e usar os dados exportados para criar relatórios.

Use a Ajuda do Active IQ Unified Manager

A Ajuda inclui informações sobre todos os recursos do Active IQ Unified Manager. Você pode usar o sumário, o índice ou a ferramenta de busca para encontrar informações sobre os recursos e como usá-los.

A ajuda está disponível em cada guia e na barra de menus da interface de 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 menus.

Você pode encontrar informações mais detalhadas expandindo qualquer parte do Sumário no painel de navegação.

- Para pesquisar o conteúdo da Ajuda, clique na guia **Pesquisar** no painel de navegação, digite a palavra ou série de palavras que você deseja encontrar e clique em **Ir!**
- Para imprimir tópicos de Ajuda, clique no ícone da impressora.

Adicione aos favoritos seus tópicos de Ajuda no Active IQ Unified Manager

Na guia Favoritos da Ajuda, você pode adicionar aos favoritos os tópicos da Ajuda que usa com frequência. Os favoritos da Ajuda proporcionam acesso rápido aos seus tópicos preferidos.

Passos

1. Navegue até o tópico de Ajuda que você deseja adicionar aos favoritos.
2. Clique em **Favoritos** e, em seguida, clique em **Adicionar**.

Pesquise objetos de armazenamento no Active IQ Unified Manager

Para acessar rapidamente um objeto específico, você pode usar o campo **Pesquisar todos os objetos de armazenamento** na parte superior da barra de menu. Esse método de pesquisa global em todos os os objetos permite localizar rapidamente objetos específicos por tipo. Os resultados da pesquisa são classificados por tipo de objeto de armazenamento e você pode filtrá-los ainda mais por objeto usando o menu suspenso.

Antes de começar

- Para executar esta tarefa, você precisa ter uma das seguintes funções: Operator, Application Administrator ou Storage Administrator.
- Uma pesquisa válida deve conter pelo menos três caracteres.

Ao usar o valor "Todos" no menu suspenso, 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 objetos. Você pode selecionar um tipo de objeto específico no menu suspenso para refinar a pesquisa em um tipo de objeto específico. Nesse caso, a lista retornada não se restringe aos 25 principais objetos.

Os tipos de objetos que você pode pesquisar incluem:

- Clusters
- Nós
- VMs de armazenamento
- Agregados
- Volumes
- Qtrees
- Compartilhamentos SMB
- Compartilhamentos NFS
- Cotas de usuário ou grupo

- LUNs
- Espaços de nomes NVMe
- Grupos de iniciadores
- Iniciadores
- Grupo de consistência

Ao inserir o nome de uma carga de trabalho, a lista de cargas de trabalho na categoria apropriada de Volumes ou LUNs é retornada.

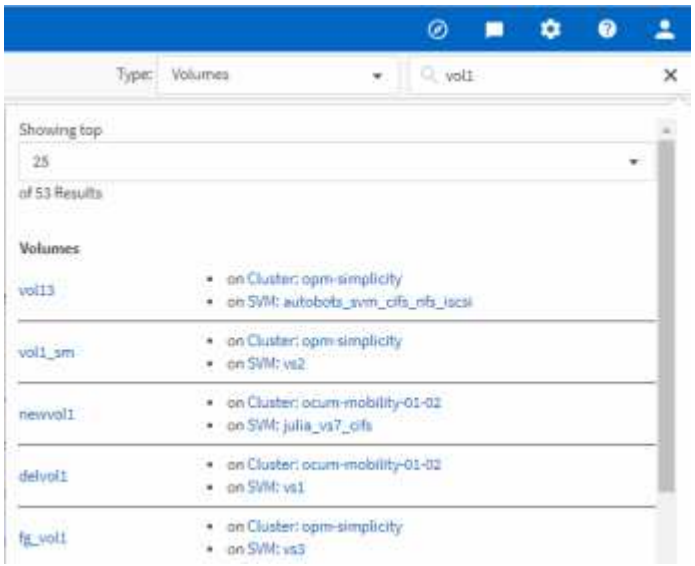
Você pode clicar em qualquer objeto nos resultados da pesquisa para navegar até a página de detalhes de integridade desse objeto. Se não houver uma página de integridade direta para um objeto, a página de integridade do objeto pai será exibida. Por exemplo, ao pesquisar um LUN específico, a página de detalhes do SVM no qual o LUN reside será exibida.

Não é possível pesquisar portas ou LIFs 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.



Exporte os dados de armazenamento como relatórios no Active IQ Unified Manager

Você pode exportar dados de armazenamento em diversos formatos de saída e, em seguida, usar os dados exportados para criar relatórios. Por exemplo, se houver 10 eventos críticos que não foram resolvidos, você pode exportar os dados da página de inventário do Gerenciamento de Eventos para criar um relatório e, em seguida, enviar o relatório aos administradores que podem resolver os problemas.

Você pode exportar dados para um `.csv`arquivo, `.xlsx`arquivo ou `.pdf`documento a partir das páginas de inventário **Armazenamento** e **Rede** e usar os dados exportados para criar relatórios. Existem outros locais no produto onde apenas `.csv` ou `.pdf` arquivos podem ser gerados.

Passos

1. Execute uma das seguintes ações:

Se você deseja exportar…	Faça isso…
Detalhes do inventário de objetos de storage	Clique em **Storage** ou **Network** no menu de navegação à esquerda e selecione um objeto de storage. Escolha uma das visualizações fornecidas pelo sistema ou qualquer visualização personalizada que você tenha criado.
Detalhes do grupo de políticas de QoS	Clique em **Armazenamento** > **Grupos de Políticas de QoS** no menu de navegação à esquerda.
Detalhes sobre a capacidade de armazenamento e o histórico de proteção	Clique em **Armazenamento** > **Agregados** ou **Armazenamento** > **Volumes** e, em seguida, selecione um único agregado ou volume.
Detalhes do evento	Clique em **Event Management** 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 de usuário).
3. Clique em **Download CSV**, **Download PDF** ou **Download Excel** para confirmar a solicitação de exportação.

   Na guia "Top Performers", você pode optar por baixar um relatório das estatísticas do cluster que está visualizando ou de todos os clusters do data center.

   O arquivo foi baixado.

4. Abra o arquivo no aplicativo adequado.

Informações relacionadas

"Página de inventário de integridade/clusters"

"Agendamento de um relatório"

Filtre o conteúdo da página de inventário no Active IQ Unified Manager

Você pode filtrar os dados da página de inventário do Unified Manager para localizar rapidamente os dados com base em critérios específicos. Você pode usar a filtragem para restringir o conteúdo das páginas do Unified Manager e mostrar apenas os resultados nos quais você tem interesse. Isso proporciona um método muito eficiente de

exibir apenas os dados nos quais você tem interesse.

Use a opção **Filtragem** para personalizar a visualização em grade de acordo com suas preferências. As opções de filtro disponíveis se baseiam no tipo de objeto visualizado na grade. Se houver filtros aplicados no momento, o número de filtros aplicados será exibido à direita do botão Filter.

Há suporte para três tipos de parâmetros de filtro.

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**.

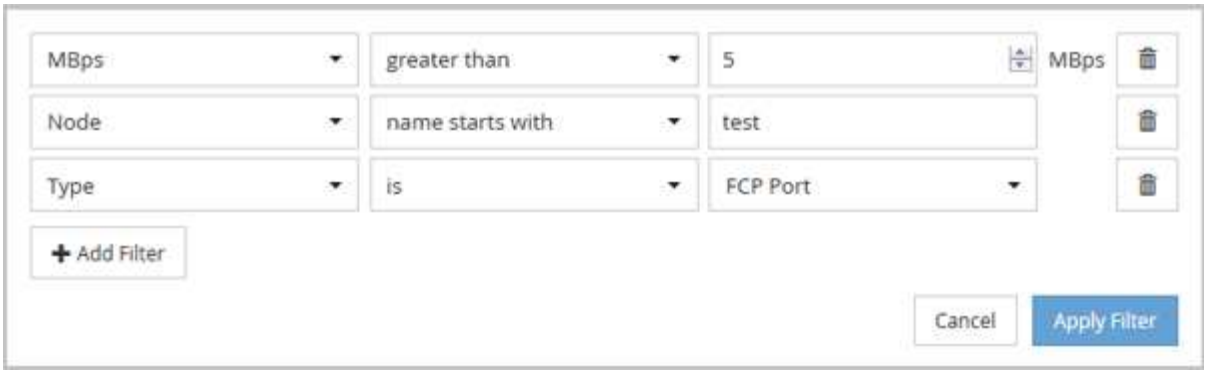
Os campos Coluna, Operador e Valor são obrigatórios para cada filtro; os filtros disponíveis refletem as colunas filtráveis na página atual. O número máximo de filtros que você pode aplicar é quatro. Os resultados filtrados são baseados na combinação dos parâmetros de filtro. Os resultados filtrados se aplicam a todas as páginas da sua pesquisa filtrada, não apenas à página exibida no momento.

Você pode adicionar filtros usando o painel de Filtragem.

1. Na parte superior da página, clique no botão **Filtrar**. O painel de 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 desse objeto.
5. Para adicionar outro filtro, clique em **+Add Filter**. Um campo de filtro adicional é exibido. Preencha este filtro usando o processo descrito nas etapas anteriores. Observe que, ao adicionar o seu quarto filtro, o botão **+Add Filter** não é 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 de filtragem para remover filtros individuais clicando no ícone da lixeira à direita do filtro que você deseja remover.
8. Para remover todos os filtros, clique em **Reset** na parte inferior do painel de filtragem.

Exemplo de filtragem

A ilustração mostra o painel de filtragem com três filtros. O botão **+Adicionar Filtro** é exibido quando você tem menos de quatro filtros, o limite máximo.



Após clicar em **Aplicar filtro**, o painel de filtragem fecha, aplica seus filtros e mostra o número de filtros aplicados (3).

Visualize os eventos ativos a partir do ícone de notificação no Active IQ Unified Manager

O ícone de sino de notificação ( ) na barra de menu fornece uma maneira rápida de visualizar os eventos ativos mais importantes que o Unified Manager está monitorando.

A lista de eventos ativos permite visualizar o número total de eventos críticos, de erro, de aviso e de atualização em todos os clusters. Essa lista inclui eventos dos últimos 7 dias e não inclui eventos de informação. Você pode clicar em um link para exibir a lista de eventos que mais interessam a você.

Observe que, quando um cluster está inacessível, o Unified Manager exibe essas informações nesta página. Você pode visualizar informações detalhadas sobre um cluster inacessível clicando no botão **Details**. Essa ação abre a página Event details. Problemas de monitoramento de escala, como pouco espaço ou RAM insuficiente na estação de gerenciamento, também são exibidos nesta página.

Passos

1. Na barra de menus, clique em .
2. Para visualizar os detalhes de qualquer um dos eventos ativos, clique no link de texto do evento, como "2 Capacity" ou "4 Performance".

Monitore e gerencie clusters a partir do painel de controle

Monitore e gerencie clusters a partir do painel de controle no Active IQ Unified Manager

O painel fornece informações cumulativas, de relance, sobre o estado atual dos seus sistemas ONTAP monitorados. O painel fornece “painéis” que permitem avaliar a capacidade geral, o desempenho e o estado de segurança dos clusters que você está monitorando.

Além disso, existem certos problemas do ONTAP que você pode corrigir diretamente na interface de usuário do Unified Manager, em vez de ter que usar o ONTAP System Manager ou a ONTAP CLI.

Na parte superior do painel de controle, você pode selecionar se os painéis exibem informações de todos os clusters monitorados ou de um cluster individual. Você pode começar visualizando o status de todos os clusters e depois aprofundar em clusters individuais quando quiser ver informações detalhadas.

Alguns dos painéis listados abaixo podem não aparecer na página dependendo da sua configuração.

Painéis	Descrição
Ações de gerenciamento	Quando o Unified Manager consegue diagnosticar e determinar uma única solução para um problema, essa solução é exibida neste painel com um botão **Fix It**.
Capacidade	Exibe a capacidade total e a capacidade utilizada da camada local e da camada de nuvem, bem como o número de dias até que a capacidade local atinja o limite máximo.
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 máximo.
IOPS da carga de trabalho	Exibe o número total de cargas de trabalho em execução no momento em um determinado intervalo de IOPS.
Desempenho da carga de trabalho	Exibe o número total de cargas de trabalho em conformidade e não conformes 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.
Proteção	Exibe o número de VMs de storage protegidas pela relação de SVM-DR, volumes protegidos pela relação do SnapMirror, volumes protegidos pelo Snapshot e clusters protegidos pelo MetroCluster.
Visão geral de uso	Exibe os clusters classificados por maior IOPS, maior taxa de transferência (MBps) ou maior capacidade física utilizada.

Saiba mais sobre a página do painel de controle do Active IQ Unified Manager

A página Dashboard tem "painéis" que exibem uma visão geral da capacidade, do desempenho e da integridade de segurança dos clusters que você está monitorando. Esta página também fornece um painel Management Actions que lista as correções que o Unified Manager pode aplicar para resolver determinados eventos.

A maioria dos painéis também exibe o número de eventos ativos nessa categoria e o número de novos eventos adicionados nas 24 horas anteriores. Essas informações ajudam você a decidir quais clusters talvez precise analisar mais para resolver os eventos. Ao clicar nos eventos, você vê os principais eventos e um link para a página de inventário do Event Management filtrada para mostrar os eventos ativos nessa categoria.

Na parte superior do painel, você pode selecionar se os painéis exibem informações de todos os clusters monitorados ("Todos os Clusters") ou de um cluster individual. Você pode começar visualizando o status de todos os clusters e, em seguida, ir para clusters individuais quando quiser ver informações detalhadas.

Alguns dos painéis listados abaixo aparecem no painel de controle dependendo da sua configuração.

Painel de ações de gerenciamento

Existem certos problemas que o Unified Manager pode diagnosticar minuciosamente e para os quais pode fornecer uma única solução. Quando disponíveis, essas soluções são exibidas neste painel com um botão **Fix It** ou **Fix All**. Você pode corrigir esses problemas imediatamente no Unified Manager, em vez de ter que usar o ONTAP System Manager ou a ONTAP CLI. Para visualizar todos os problemas, clique em Ver "Corrija problemas do ONTAP diretamente do Unified Manager" para obter mais informações.

Painel de capacidade

Ao visualizar todos os clusters, este painel exibe a capacidade física usada (após aplicar a economia de eficiência de storage) e a capacidade física disponível (sem incluir a economia potencial de eficiência de storage) de cada cluster, o número de dias até que os discos fiquem cheios, conforme a projeção, e a taxa de redução de dados (sem cópias Snapshot) com base nas configurações de eficiência de storage do ONTAP. Ele também lista a capacidade usada de quaisquer camadas de nuvem configuradas. Clicar no gráfico de barras leva você à página de inventário de agregados desse cluster. Clicar no texto "Days To Full" 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 para os volumes que utilizam 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 à página de inventário de nós desse cluster. Observe que a página de inventário de nós exibe a capacidade de desempenho média das últimas 72 horas. Clicar no texto "Dias até a capacidade máxima" exibe uma mensagem que identifica o nó com o menor número de dias restantes de capacidade de desempenho; clique no nome do nó para ver mais detalhes.

Ao visualizar um único cluster, este painel exibe a porcentagem utilizada da capacidade de desempenho do cluster, o total de IOPS e a taxa de transferência total (MB/s), além do número de dias previsto para que cada uma dessas três métricas atinja seu limite máximo.

Painel de IOPS da 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 conformes 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 uma barra do gráfico leva você às cargas de trabalho em conformidade atribuídas a essa política na página Workloads. Clicar no número que segue a barra do gráfico leva você às cargas de trabalho em conformidade e não conformes atribuídas a essa política.

Painel de segurança

O painel Segurança apresenta o status de segurança de alto nível de todos os clusters ou de 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 visualizar os detalhes na página de detalhes do evento
- o status de segurança do cluster (contagem de clusters em conformidade e não conformes)
- o status de segurança da VM de armazenamento (contagem de VMs de armazenamento em conformidade e em não conformidade)
- o status de criptografia do volume (contagem dos volumes criptografados ou não criptografados)
- o status de anti-ransomware do volume (contagem de volumes com anti-ransomware ativado ou desativado)

Você pode clicar nos gráficos de barras dos clusters e das VMs de storage em conformidade e em não conformidade, dos volumes criptografados e não criptografados e do status de anti-ransomware dos volumes para acessar as respectivas páginas e visualizar os detalhes de segurança dos clusters, das VMs de storage e dos volumes filtrados.

A conformidade é baseada no "NetApp Guia de Reforço de Segurança para o ONTAP 9". Clique na seta para a direita na parte superior do painel para visualizar os detalhes de segurança de todos os clusters na página Security. Para obter informações, consulte "Visualização do status de segurança detalhado para clusters e VMs de storage".

Painel de proteção de dados

Este painel exibe o resumo da proteção de dados para um único cluster ou para todos os clusters em um data center. Ele mostra o número total de eventos de proteção de dados, eventos do MetroCluster e o número de eventos ativos gerados nas últimas 24 horas no ONTAP. Clicar no link de cada um desses eventos leva você à página de detalhes do evento. Você pode clicar no link **Ver 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 em todos os clusters em um data center protegidos por cópias Snapshot.
- O número de volumes em um cluster ou em todos os clusters em um data center protegidos por relacionamentos do SnapMirror. Para os relacionamentos do SnapMirror, considera-se a contagem de volume no cluster de origem.
- O número de clusters ou de todos os clusters em um data center protegidos por uma configuração do MetroCluster por IP ou FC.
- O número de relacionamentos de volume com atraso do objetivo de ponto de recuperação (RPO) do SnapMirror, com base no status do atraso.

Você pode passar o cursor do 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 único cluster ou de todos os clusters na página Data Protection. Você também pode clicar em:

- Os gráficos de barras de volumes desprotegidos e volumes protegidos por cópias Snapshot levam você à página Volumes, onde você pode ver os detalhes.
- Os gráficos de barras dos clusters protegidos ou não protegidos pela configuração do MetroCluster podem ser visualizados na página Clusters para ver os detalhes.
- Os gráficos de barras de todos os relacionamentos levam você à página Relacionamentos, onde os

detalhes são filtrados com base no cluster de origem.

Para obter mais informações, consulte "Visualizando o status de proteção do volume".

Painel de visão geral de uso

Ao visualizar todos os clusters, você pode optar por exibi-los classificados por maior IOPS, maior taxa de transferência (MB/s) ou maior capacidade física utilizada.

Ao visualizar um único cluster, você pode optar por visualizar as cargas de trabalho classificadas por maior IOPS, maior taxa de transferência (MB/s) ou maior capacidade lógica utilizada.

Informações relacionadas

"Corrigindo problemas usando as correções 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 / integridade"

"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 Performance Cluster Landing page"

"Monitore o desempenho usando as páginas de Inventário de Desempenho"

Corrija ou gerencie problemas do ONTAP diretamente do Unified Manager

Gerencie problemas ou recursos do ONTAP diretamente do Active IQ 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 precisar usar o ONTAP System Manager ou a CLI do ONTAP. A opção "Management Actions" fornece correções para vários problemas do ONTAP que acionaram eventos do Unified Manager.

Você pode corrigir problemas diretamente na página Management Actions, selecionando a opção **Management Actions** no painel de navegação esquerdo. As Management Actions também estão disponíveis no painel Management Actions no Dashboard, na página Event details e na seleção Workload Analysis no menu de navegação à esquerda.

Há certos problemas que o Unified Manager pode diagnosticar minuciosamente e para os quais pode fornecer uma única solução. Para certos recursos do ONTAP, como o monitoramento anti-ransomware, o Unified Manager realiza verificações internas e recomenda ações específicas. Quando disponíveis, essas soluções são exibidas em Management Actions com um botão **Fix It**. Clique no botão **Fix It** para corrigir o problema. Você deve ter a função Application Administrator ou Storage Administrator.

O Unified Manager envia comandos do ONTAP ao cluster para realizar a correção solicitada. Quando a correção é concluída, o evento se torna 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 do volume cheio", que você pode resolver clicando na ação de gerenciamento **Corrigir tudo** para "Ativar volume com crescimento automático". Com um único 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 "Que problemas o Unified Manager pode resolver".

Saiba mais sobre as opções de botão "Corrigir" e "Corrigir tudo" no Active IQ Unified Manager

A página Ações de gerenciamento oferece o botão **Corrigir** ou **Corrigir tudo** para solucionar problemas sobre os quais o Unified Manager notificou você por meio de um evento.

Recomendamos que você clique nos botões para corrigir o 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
Solicite ao Unified Manager que corrija 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 exibir todas as ações individuais de **Fix It**.Em seguida, siga as etapas para corrigir ou descartar ações de gerenciamento individuais.

O que você quer fazer?	Ação
Solicite ao Unified Manager que corrija o problema.	Clique no botão **Fix It**.
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 **Dispensar**.
Exiba os detalhes deste evento para que você possa entender melhor o problema.	• Clique no botão **Fix It** e revise a correção que será aplicada na caixa de diálogo resultante. • Clique na seta para baixo e clique em **Ver detalhes do evento** para exibir a página de detalhes do evento. Em seguida, clique em **Fix It** em qualquer uma destas páginas resultantes se quiser corrigir o problema.

O que você quer fazer?	Ação
Exiba os detalhes deste objeto de storage para que você possa entender melhor o problema.	Clique no nome do objeto de armazenamento para exibir os detalhes na página Performance Explorer ou na página Health Details.

Em alguns casos, a correção aparece na próxima verificação de configuração de 15 minutos. Em outros casos, pode levar muitas horas para que a alteração de configuração seja verificada e para que o evento seja marcado como obsoleto.

Para ver a lista de ações de gerenciamento concluídas ou em andamento, clique no ícone de filtro e selecione **Concluídas** ou **Em andamento**.

As operações do Fix All são executadas em série, portanto, ao visualizar o painel **In Progress**, alguns objetos terão o status **In Progress**, enquanto outros terão o status **Scheduled**; isso significa que eles ainda estão aguardando implementação.

Veja o status das ações de gerenciamento a serem corrigidas no Active IQ Unified Manager

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 exibida como **Concluída** rapidamente depois que o Unified Manager envia o comando ONTAP para o cluster. No entanto, algumas ações, como mover um volume, podem levar mais tempo.

Há três filtros disponíveis na página Management Actions:

- **Concluído** mostra tanto as ações de gerenciamento que foram concluídas com sucesso quanto as que falharam. As ações com **Falha** fornecem o motivo da falha para que você possa resolver o problema manualmente.
- **Em andamento** mostra tanto as ações de gerenciamento que estão em implementação quanto as que estão programadas para implementação.
- **Recomendado** mostra todas as ações de gerenciamento que estão atualmente ativas para todos os clusters monitorados.

Passos

1. Clique em **Management Actions** no painel de navegação à esquerda. Como alternativa, clique em ⋮ na parte superior do painel **Management Actions** no **Dashboard** e selecione a View que você deseja ver.

   A página Ações de gerenciamento é exibida.

2. Você pode clicar no ícone de seta 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 essa mesma finalidade.
4. Se você quiser visualizar 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 seta ao lado da ação de gerenciamento. Nessa página, há um botão **Corrigir**.

Saiba mais sobre os problemas do ONTAP que o Active IQ Unified Manager pode resolver

Ao utilizar o recurso de correção automática do Active IQ Unified Manager, você pode optar por resolver determinados problemas do ONTAP ou gerenciar certos recursos do ONTAP, como o monitoramento antiransomware, de forma eficaz por meio do Unified Manager.

Esta tabela descreve estes problemas ou recursos do ONTAP que você pode gerenciar diretamente por meio do botão **Corrigir** ou **Corrigir tudo** na interface web do Unified Manager.

Nome e descrição do evento	Ação de gerenciamento	Operação "Fix It"
Espaço do volume esgotado O volume está quase sem espaço e ultrapassou o limite de capacidade máxima. Esse limite é definido por padrão em 90% do tamanho do volume.	Ativar volume com crescimento automático	O Unified Manager determina que o volume com crescimento automático não está configurado para este volume, portanto habilita esse recurso para que o volume aumente sua capacidade quando necessário.
Inodes cheios Este volume ficou sem inodes e não pode aceitar nenhum arquivo novo.	Aumentar o número de inodes no volume	Aumenta o número de inodes no volume em 2%.
Incompatibilidade na política de camadas de armazenamento detectada O volume contém muitos dados inativos e a política de armazenamento em camadas atual está definida como "snapshot-only" ou "none".	Ativar o armazenamento em camadas automático na nuvem	Como o volume já reside em um FabricPool, ele altera a política de tiering para "auto" para que os dados inativos sejam movidos para a camada de nuvem de menor custo.
Detectada incompatibilidade de nível de armazenamento O volume tem muitos dados inativos, mas não reside em uma camada de armazenamento habilitada para nuvem (FabricPool).	Alterar a camada de armazenamento dos volumes	Move o volume para a camada de armazenamento habilitada para nuvem e define a política de disposição em camadas como "auto" para mover os dados inativos para a camada de nuvem.
Log de auditoria desativado O log de auditoria não está habilitado para a VM de armazenamento	Ative o registro de auditoria para a VM de armazenamento	Habilita o log de auditoria na máquina virtual de armazenamento. Observe que a máquina virtual de armazenamento já deve ter um local de log de auditoria local ou remoto configurado.

Nome e descrição do evento	Ação de gerenciamento	Operação "Fix It"
Banner de login desativado O banner de login do cluster deve ser ativado para aumentar a segurança deixando as restrições de acesso claras.	Defina o banner de login para o cluster	Define o banner de login do cluster como “Acesso restrito a usuários autorizados”.
Banner de login desativado O banner de login da VM de armazenamento deve ser ativado para aumentar a segurança, deixando claras as restrições de acesso.	Defina o banner de login para a máquina virtual de armazenamento	Define o banner de login da VM de armazenamento como "Acesso restrito a usuários autorizados".
O SSH está usando cifras inseguras Cifras com o sufixo "-cbc" são consideradas inseguras.	Remova as cifras inseguras do cluster	Remove as cifras inseguras, como aes192-cbc e aes128-cbc, do cluster.
O SSH está usando cifras inseguras Cifras com o sufixo "-cbc" são consideradas inseguras.	Remova as cifras inseguras da máquina virtual de armazenamento	Remove as cifras inseguras — como aes192-cbc e aes128-cbc — da VM de armazenamento.
AutoSupport transporte HTTPS desativado O protocolo de transporte usado para enviar mensagens do AutoSupport ao suporte técnico deve ser criptografado.	Defina o HTTPS como protocolo de transporte para mensagens do AutoSupport	Define o HTTPS como o protocolo de transporte para mensagens do AutoSupport no cluster.
Limiar de desequilíbrio de carga do cluster ultrapassado Indica que a carga está desequilibrada entre os nós do cluster. Este evento é gerado quando a variação na capacidade de desempenho utilizada entre os nós é superior a 30%.	Equilibre as cargas de trabalho do cluster	O Unified Manager identifica o melhor volume para mover de um nó para o outro a fim de reduzir o desequilíbrio e, em seguida, move o volume.
Limiar de desequilíbrio de capacidade do cluster ultrapassado Indica que a capacidade está desequilibrada entre os agregados no cluster. Este evento é gerado quando a variação da capacidade utilizada entre os agregados é superior a 70%.	Equilibre a capacidade do cluster	O Unified Manager identifica o melhor volume a ser transferido de um agregado para outro para reduzir o desequilíbrio e, em seguida, realiza a transferência.

Nome e descrição do evento	Ação de gerenciamento	Operação "Fix It"
Limite de capacidade de desempenho usada excedido Indica que a carga no nó pode ficar sobrecarregada 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 utilizada do nó é superior a 100% por mais de 12 horas.	Limitar a alta carga no nó	O Unified Manager identifica o volume com o maior número de IOPS e aplica uma política de QoS usando os níveis históricos de IOPS esperados e de pico para reduzir a carga no nó.
Limiar de alerta de evento dinâmico ultrapassado Indica que o nó já está operando em estado de sobrecarga devido à carga anormalmente alta de algumas das cargas de trabalho.	Reduzir a sobrecarga no nó	O Unified Manager identifica o volume com o maior número de IOPS e aplica uma política de QoS usando os níveis históricos de IOPS esperados e de pico para reduzir a carga no nó.
A tomada de controle não é possível O failover está desativado no momento, portanto o acesso aos recursos do nó durante uma interrupção ou reinicialização será perdido até que o nó fique disponível novamente.	Habilitar failover de nó	O Unified Manager envia o comando apropriado para habilitar o failover em todos os nós do cluster.
A opção Cf.takeover.on_panic está configurada como OFF A opção do nodeshell "cf.takeover.on_panic" está definida como **desativada**, o que pode causar problemas em sistemas configurados com HA.	Habilitar a tomada de controle em caso de pânico	O Unified Manager envia o comando apropriado ao cluster para alterar essa configuração para **ativada**.
Desative 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 off	O Unified Manager envia o comando apropriado ao cluster para alterar essa configuração para **desativada**.

Nome e descrição do evento	Ação de gerenciamento	Operação "Fix It"
Telnet habilitado Indica um potencial problema de segurança porque o Telnet é inseguro e transmite dados sem criptografia.	Desativar Telnet	O Unified Manager envia o comando apropriado ao cluster para desativar o Telnet.
Configurar o aprendizado anti-ransomware da VM de armazenamento Verifica periodicamente se há 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 `learning` modo de monitoramento anti-ransomware	O Unified Manager configura o monitoramento antiransomware para o estado `learning` nas VMs de armazenamento por meio do console de gerenciamento de clusters. O monitoramento antiransomware em todos os novos volumes criados na VM de armazenamento é automaticamente movido para o modo de aprendizado. Com essa capacitação, o ONTAP pode aprender o padrão de atividade nos volumes e detectar anomalias devido a possíveis ataques maliciosos.
Configurar o aprendizado anti-ransomware do volume Verifica periodicamente se existem clusters com licenças para monitoramento anti-ransomware. Valida se um volume suporta apenas serviços NFS ou SMB em tal cluster.	Coloque os volumes em `learning` modo de monitoramento anti-ransomware	O Unified Manager define o monitoramento antirransomware para o estado `learning` nos volumes por meio do console de gerenciamento de clusters. Com essa capacitação, o ONTAP consegue aprender o padrão de atividade nos volumes e detectar anomalias decorrentes de possíveis ataques maliciosos.
Ativar proteção contra ransomware por volume Verifica periodicamente se há clusters com licenças para monitoramento anti-ransomware. Detecta se os volumes estão no `learning` modo de monitoramento anti-ransomware por mais de 45 dias e determina a possibilidade de colocá-los no modo ativo.	Coloque os volumes no `active` modo de monitoramento anti-ransomware	O Unified Manager configura o monitoramento antiransomware para `active` nos volumes por meio do console de gerenciamento de clusters. Com essa capacitação, 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.

Nome e descrição do evento	Ação de gerenciamento	Operação "Fix It"
Desativar a proteção contra ransomware do volume Verifica periodicamente se existem 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).	Desative o monitoramento anti-ransomware nos volumes	O Unified Manager desativa o monitoramento anti-ransomware nos volumes por meio do console de gerenciamento de clusters.

Substitua as ações de gerenciamento com scripts no Active IQ Unified Manager

Você pode criar scripts personalizados e associá-los a alertas para executar ações específicas para eventos específicos, em vez de optar pelas ações de gerenciamento padrão disponíveis para eles na página Management Actions ou no dashboard 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 ações de gerenciamento fornecido pelo Unified Manager, poderá configurar um script personalizado para a ação específica. Em seguida, você poderá associar o script a um alerta para esse tipo de evento e cuidar desses eventos individualmente. Nesse caso, as ações de gerenciamento não são geradas para esse tipo de evento específico na página Management Actions ou no painel do Unified Manager.

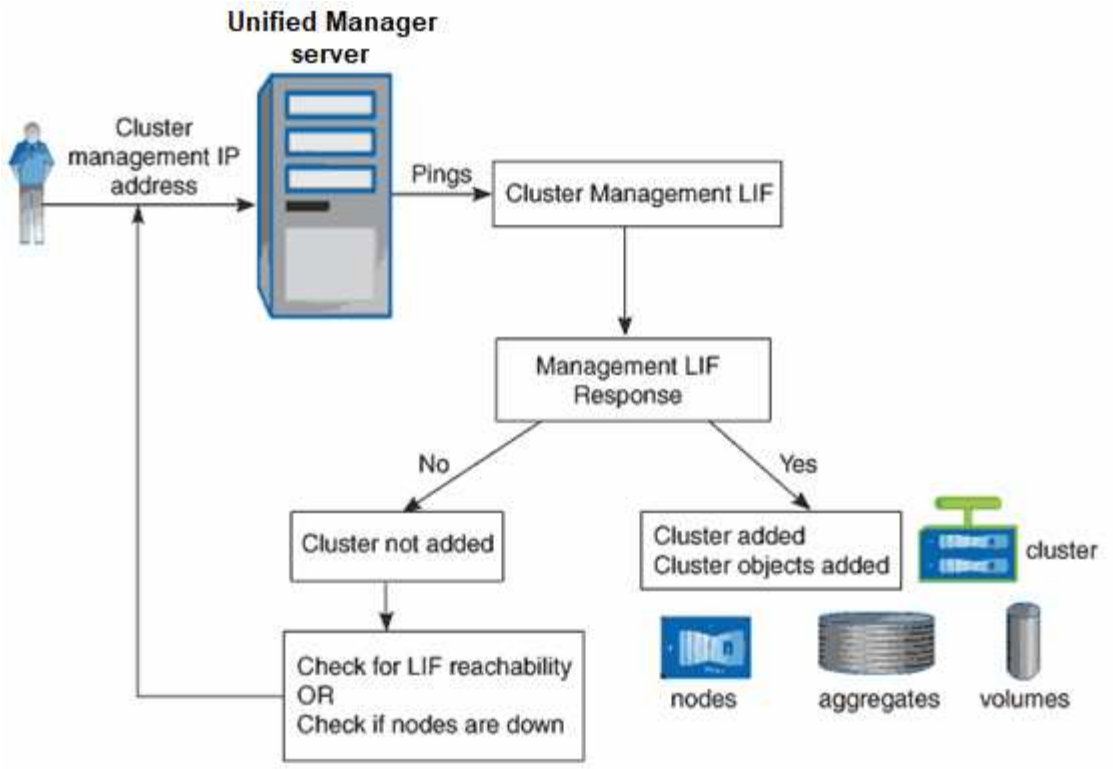
Gerencie clusters

Aprenda como funciona o processo de descoberta de clusters no Active IQ Unified Manager

Depois de adicionar um cluster ao Unified Manager, o servidor descobre os objetos do cluster e os adiciona ao seu banco de dados. Compreender como funciona o processo de descoberta ajuda você a gerenciar os clusters da sua organização e seus respectivos objetos.

O intervalo de monitoramento para coletar informações de configuração do cluster é de 15 minutos. Por exemplo, depois que você adiciona um cluster, leva 15 minutos para exibir os objetos do cluster na UI do Unified Manager. Esse intervalo de tempo também se aplica quando você faz alterações em um cluster. Por exemplo, se você adicionar dois novos volumes a uma SVM em um cluster, verá esses novos objetos na UI após o próximo intervalo de polling, que pode levar até 15 minutos.

A imagem a seguir ilustra o processo de descoberta:



Após todos os objetos de um novo cluster serem 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. Esse recurso fornece a você mais de duas semanas de informações de desempenho de um cluster imediatamente após sua adição. 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 muito da 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.

Veja a lista de clusters monitorados pelo Active IQ Unified Manager

Você pode usar a página de Configuração de Cluster para visualizar seu inventário de clusters. Você pode ver detalhes sobre os clusters, como nome ou endereço IP e status de comunicação.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Etapa

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de cluster**.

   Todos os clusters no seu ambiente de storage gerenciado pelo Unified Manager são exibidos. A lista de clusters é classificada pela coluna de nível de severidade do estado da coleta. Você pode clicar no cabeçalho de uma coluna para classificar os clusters por diferentes colunas.

Adicionar clusters ao Active IQ Unified Manager

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

Antes de começar

- Você precisa ter a função de Administrador de Aplicativos ou a função de Administrador de Armazenamento.
- Você precisa ter as seguintes informações:
  - O Unified Manager oferece suporte a clusters ONTAP locais, ao ONTAP Select e ao Cloud Volumes ONTAP.
  - Você precisa ter o nome do host ou o endereço IP de gerenciamento de cluster (IPv4 ou IPv6) do cluster.

    Ao usar o nome do host, ele deve ser resolvido para o endereço IP de gerenciamento do cluster da LIF de gerenciamento do cluster. Se você usar uma LIF de gerenciamento de nó, a operação falhará.
  - Você precisa do nome de usuário e da senha para acessar o cluster.

    Esta conta deve ter a função *admin* com acesso ao aplicativo definido como *ontapi*, *amqp*, *console* e *http*.
  - Você precisa saber o número da porta para se conectar ao cluster usando o protocolo HTTPS (normalmente a porta 443).
  - O cluster deve estar executando o software ONTAP versão 9.9 ou superior.
  - Você deve ter espaço suficiente no servidor do Unified Manager. A adição de um cluster ao servidor fica impedida quando mais de 90% do espaço já estiver ocupado.
  - Você possui os certificados necessários:

    Certificado SSL (HTTPS): este certificado pertence ao Unified Manager. Um certificado SSL (HTTPS) autoassinado padrão é gerado com uma nova instalação do Unified Manager. NetApp recomenda que você o 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 como regenerar o certificado SSL, consulte "Gerando um certificado de segurança HTTPS".

    Certificado EMS: Este certificado pertence ao Unified Manager. Ele é usado durante a autenticação para notificações EMS recebidas do ONTAP.

    Certificados para comunicação TLS mútua: utilizados durante a comunicação TLS mútua entre o Unified Manager e o ONTAP. A autenticação baseada em certificado é habilitada para um cluster, dependendo da versão do ONTAP. Se o cluster que executa a versão do ONTAP for inferior a 9.5, a autenticação baseada em certificado não será habilitada.

    A autenticação baseada em certificado não é habilitada automaticamente para um cluster se você estiver atualizando uma versão mais antiga do Unified Manager. No entanto, você pode habilitá-la 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 pela interface de usuário da web, e a autenticação baseada em certificado é ativada automaticamente.
- Você pode adicionar um cluster pela CLI do Unified Manager; a autenticação baseada em certificado não está habilitada por padrão. Se você adicionar um cluster usando a CLI do Unified Manager, precisará editar o cluster usando a interface do usuário do Unified Manager. Consulte "Comandos da CLI do Unified Manager suportados" para adicionar um cluster usando a CLI do Unified Manager.
- Se a autenticação baseada em certificado estiver habilitada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurá-lo em outro servidor do Unified Manager em que o nome do host ou o endereço IP foi alterado, o monitoramento do cluster poderá falhar. Para evitar essa falha, edite e salve os detalhes do cluster. Para obter mais informações sobre como editar os 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 pertence ao ONTAP. Não é possível adicionar um cluster ao Unified Manager com um certificado expirado e, caso o certificado já tenha expirado, você deve regenerá-lo antes de adicionar o cluster. Para obter informações sobre a geração de certificados, consulte o artigo da base de conhecimento (KB) "Como renovar um certificado autoassinado do 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 o número de nós suportado, precisará instalar uma instância adicional do Unified Manager para monitorar alguns dos clusters. Para ver a lista do número de nós suportado, 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 de 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 Authorize Host, clique em **View Certificate** para visualizar as informações do certificado do cluster.
5. Clique em **Yes**.

   Após salvar os detalhes do cluster, você poderá visualizar o certificado para a comunicação TLS mútua de um cluster.

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

Após todos os objetos de um novo cluster serem 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. Esse recurso fornece a você mais de duas semanas de informações de desempenho de um cluster imediatamente após sua adição. 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. 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 referentes ao período ausente.
- Ao adicionar um cluster ONTAP com a versão 9.14.1 ou posterior, a comunicação ocorre por meio do recurso de agente de nuvem. O ONTAP cria automaticamente um usuário de conta de serviço interna com privilégios somente de leitura (por exemplo, clus-agent-xxxx). O Unified Manager para de coletar dados desses clusters se o `clus-agent` usuário for excluído.

Se você receber uma mensagem de erro informando que não é possível adicionar o cluster, verifique se há algum dos seguintes problemas:

- Se os relógios dos 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 o 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 e os detalhes dos clusters"

"Instalando um certificado HTTPS assinado e retornado por uma Autoridade Certificadora (CA)"

Edite as configurações do cluster no Active IQ Unified Manager

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 Edit Cluster.

Antes de começar

Você precisa 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 somente usando 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 **Edit 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 Mutual TLS, com base na versão do ONTAP. Para obter mais informações sobre a versão do ONTAP, consulte "Certificados para comunicação TLS mútua". + Você pode visualizar os detalhes do certificado clicando em **Certificate Details**. Se o certificado estiver expirado, clique no botão **Regenerate** para incorporar o novo certificado.

4. Clique em **Enviar**.
5. Na caixa de diálogo Authorize Host, clique em **View Certificate** para visualizar as informações do certificado do cluster.
6. Clique em **Yes**.

Informações relacionadas

"Adicionando usuários"

"Visualizando a lista e os detalhes dos clusters"

Remover clusters do Active IQ Unified Manager

Você pode remover um cluster do Unified Manager usando a página Cluster Setup. Por exemplo, você pode remover um cluster se a descoberta do cluster falhar ou quando quiser desativar um sistema de storage.

Antes de começar

Você precisa ter a função de Administrador de Aplicativos ou a função de Administrador de Armazenamento.

Esta tarefa remove o cluster selecionado do Unified Manager. Após a remoção, o cluster deixa de ser monitorado. A instância do Unified Manager registrada no cluster removido também é desregistrada do cluster.

A remoção de um cluster também exclui todos os seus objetos de storage, dados históricos, serviços de storage e todos os eventos associados do Unified Manager. Essas alterações aparecem nas páginas de inventário e nas páginas de detalhes após o próximo ciclo de coleta de dados.

> Você deve remover um cluster do Unified Manager antes de desativá-lo. Se o cluster já estiver offline ou inacessível quando você tentar removê-lo, o Unified Manager não poderá se comunicar com o cluster para remover o registro do aplicativo e as assinaturas do Event Management System (EMS) configuradas. Isso fará com que o processo de remoção falhe ou pare de responder antes da conclusão.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de cluster**.
2. Na página Cluster Setup, selecione o cluster que deseja remover e clique em **Remove**.
3. Na caixa de diálogo **Remover Fonte de Dados**, clique em **Remover** para confirmar a solicitação de remoção.

Informações relacionadas

"Adicionando usuários"

"Visualizando a lista e os detalhes dos clusters"

Redescubra clusters no Active IQ Unified Manager

Você pode redescobrir manualmente um cluster na página Cluster Setup 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 desejar que o Unified Manager detecte as alterações que você fizer.

Quando o Unified Manager é emparelhado com o OnCommand Workflow Automation (WFA), esse emparelhamento 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 e os detalhes dos clusters"

Monitorar a infraestrutura virtual VMware

Entenda como o Active IQ Unified Manager monitora a infraestrutura virtual VMware

O Active IQ Unified Manager oferece visibilidade das máquinas virtuais (VMs) na sua infraestrutura virtual e permite monitorar e solucionar problemas de storage e desempenho no seu ambiente virtual. Você pode usar esse recurso para identificar problemas de latência no seu ambiente de storage 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 as camadas de computação, rede e storage. Qualquer atraso no desempenho de uma aplicação em uma máquina virtual pode ocorrer devido a uma combinação de latências enfrentadas pelos vários componentes em suas respectivas camadas. Esse recurso é útil para administradores de storage e do vCenter Server, bem como para 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 pelo menu vCenter da seção VMware. A visualização rápida de cada máquina virtual listada tem o link **VCENTER SERVER** na **TOPOLOGY VIEW**, que abre o vCenter Server em um novo navegador. Você também pode usar o botão **Expand Topology** para abrir o vCenter Server e clicar no botão **View in vCenter** para ver os datastores 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 storage. A visão também destaca o objeto específico que causa a lentidão no desempenho, permitindo que você tome medidas corretivas e resolva o problema subjacente.

Uma infraestrutura virtual implantada no storage ONTAP inclui os seguintes objetos:

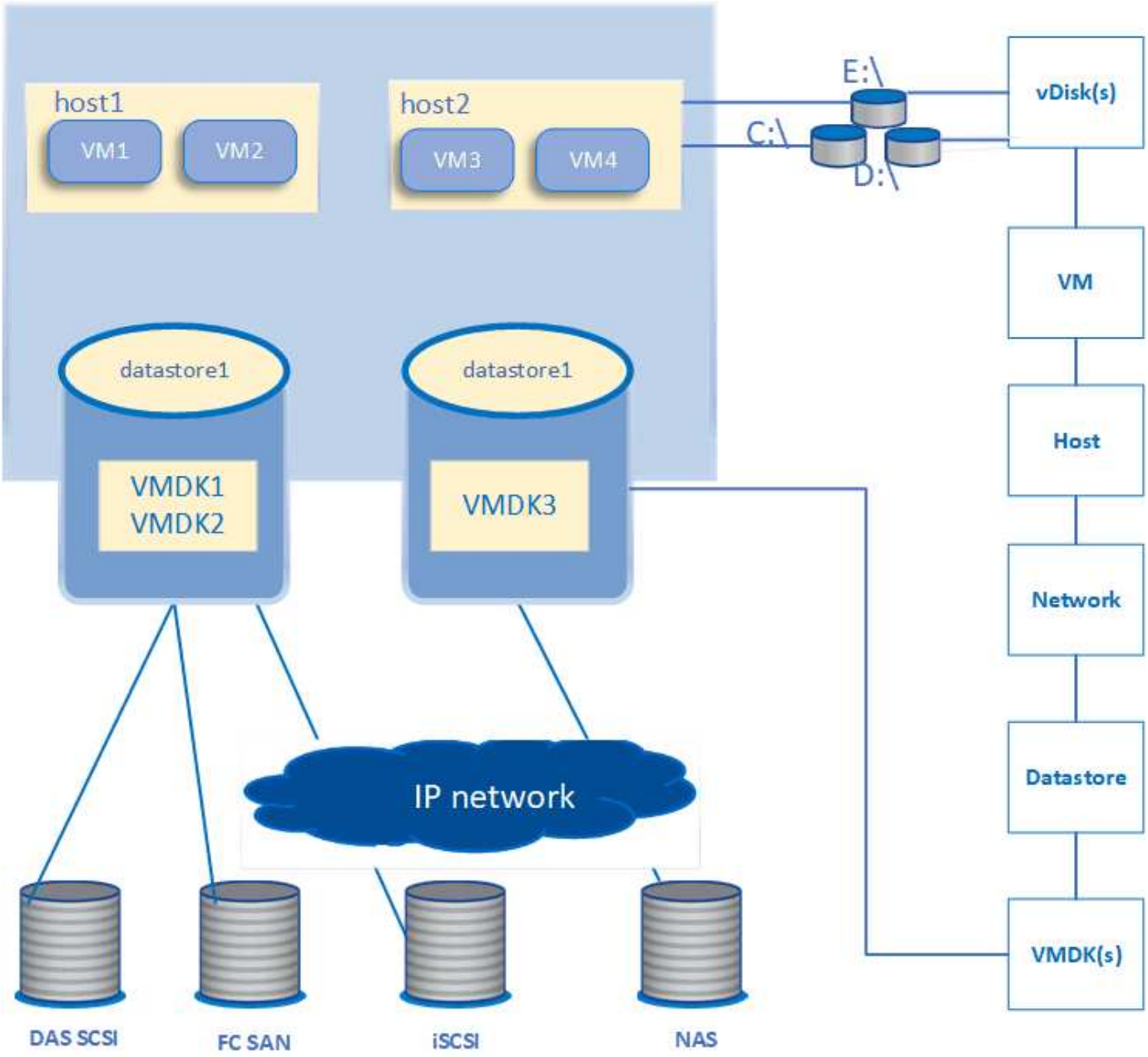
- O vCenter Server: um plano de controle centralizado para gerenciar as VMs do VMware, os hosts ESXi e

todos os componentes relacionados em um ambiente virtual. Para obter mais informações sobre o vCenter Server, consulte a documentação da VMware.

- Host: um sistema físico ou virtual que executa o ESXi, o software de virtualização da VMware, e hospeda a VM.
- Datastore: os datastores são objetos de storage virtual conectados aos hosts ESXi. Os datastores são entidades de storage gerenciáveis do ONTAP, como LUNs ou volumes, usadas como repositório para arquivos de máquina virtual, 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 datastores fora do ONTAP que são mapeados para o vCenter Server não são compatíveis nem exibidos no Unified Manager.
- VM: uma máquina virtual VMware.
- Discos virtuais: os discos virtuais nos datastores pertencentes às VMs que têm a extensão VMDK. Os dados de um disco virtual são armazenados no VMDK correspondente.
- VMDK: um disco de máquina virtual no datastore que fornece espaço de storage para discos virtuais. Para cada disco virtual, existe um VMDK correspondente.

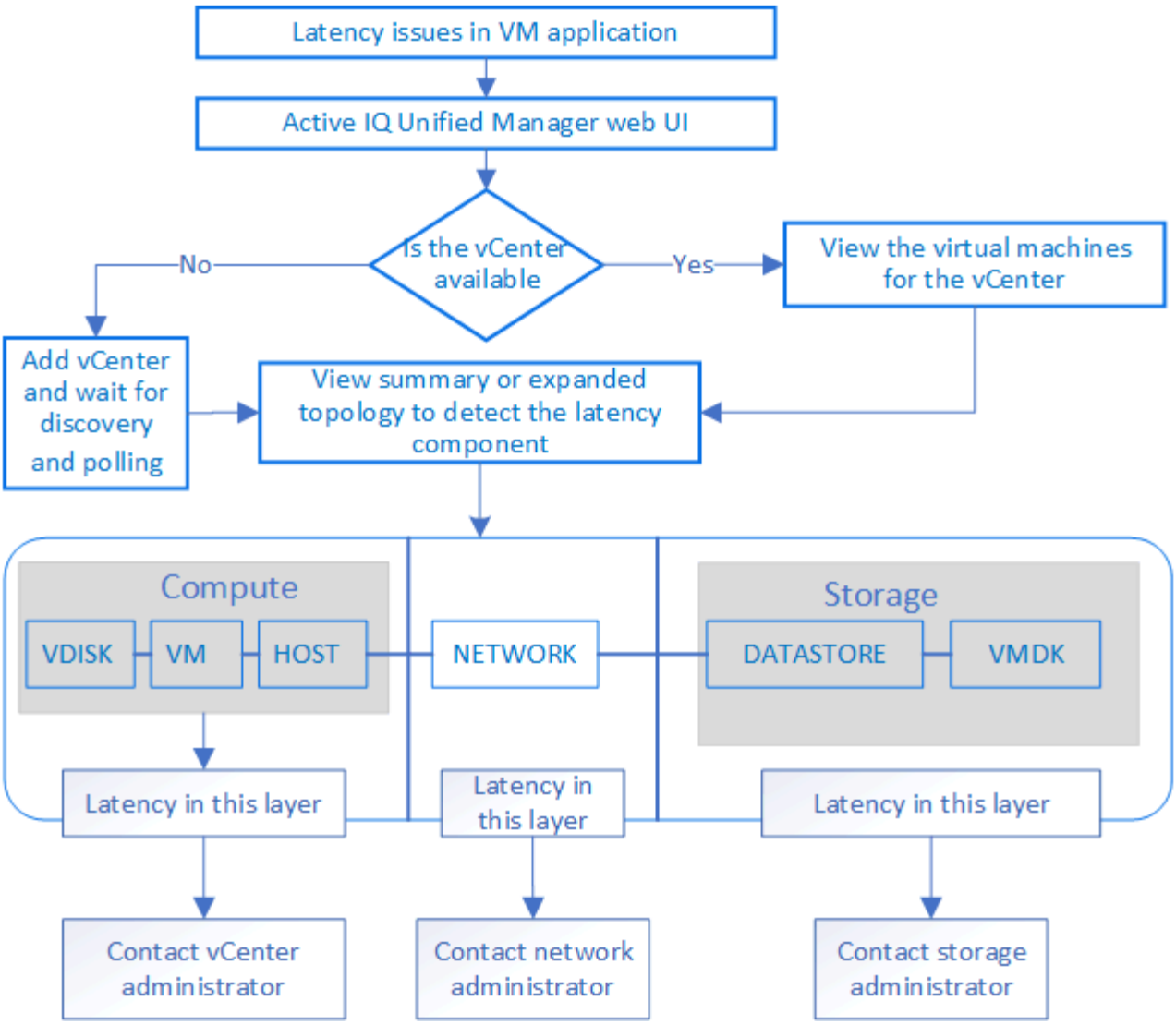
Esses objetos são representados em uma visualização de topologia de VM.

virtualização VMware no ONTAP



Fluxo de trabalho do usuário

O diagrama a seguir exibe um caso de uso típico da visualização da topologia da VM:



O que não é suportado

- Os datastores que estão fora do ONTAP e são mapeados para as instâncias do servidor vCenter não são suportados no Unified Manager. Quaisquer VMs com discos virtuais nesses datastores também não são suportadas.
- Não há suporte para um datastore que abranja várias LUNs.
- Não há suporte para datastores que usam Network address translation (NAT) para o mapeamento de LIFs de dados (endpoint de acesso).
- Não há suporte para exportar volumes ou LUNs como datastores em clusters diferentes com os mesmos endereços IP em uma configuração de múltiplas LIFs, pois o Unified Manager não consegue identificar a qual cluster cada datastore pertence.

  Exemplo: suponha que o cluster A tenha o datastore A. O datastore A é exportado via LIF de dados com o mesmo endereço IP x.x.x.x e a VM A é criada nesse datastore. Da mesma forma, o cluster B tem o datastore B. O datastore B é exportado via LIF de dados com o mesmo endereço IP x.x.x.x e a VM B é criada no datastore B. O UM não conseguirá mapear o datastore A da topologia da VM A para o volume/LUN correspondente do ONTAP, nem mapear a VM B.

- Apenas volumes NAS e SAN (iSCSI e FCP para VMFS) são suportados como datastores, 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 que você gere relatórios para analisar o desempenho dos vários componentes.
- Para a configuração de recuperação de desastres (DR) da máquina virtual de storage (VM de storage), que é compatível apenas com a infraestrutura virtual no Unified Manager, a configuração precisa ser alterada manualmente no servidor vCenter para apontar para os LUNs ativos em cenários de switchover e switchback. Sem intervenção manual, seus datastores ficam inacessíveis.

Visualize e adicione servidores vCenter no Active IQ Unified Manager

Para visualizar e solucionar problemas de desempenho das máquinas virtuais (VMs), os servidores vCenter associados devem ser adicionados à sua instância do Active IQ Unified Manager.

Antes de começar

Antes de adicionar ou visualizar servidores vCenter, certifique-se do seguinte:

- Você conhece os nomes dos servidores vCenter.
- Você conhece o endereço IP do vCenter Server e possui 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 está definida para o nível de estatísticas `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 “Data Collection Levels” do *vSphere Monitoring and Performance Guide* na documentação da VMware.

- Os valores de latência no vCenter Server são configurados em milissegundos, e não em microssegundos, para calcular os valores de latência com sucesso.
- Ao adicionar o datastore ao servidor vCenter Server, você pode usar tanto o endereço IP do host quanto o domínio totalmente qualificado (FQDN). Caso você esteja adicionando o FQDN, certifique-se de que o nome de domínio possa ser resolvido pelo servidor Unified Manager. Por exemplo, em uma instalação do Linux, certifique-se de que o nome de domínio seja adicionado ao arquivo `/etc/resolv.conf`.
- A hora atual do vCenter Server está sincronizada com o fuso horário do vCenter Server.
- O servidor vCenter está acessível para uma descoberta bem-sucedida.
- Você tem acesso de leitura ao VMware SDK ao adicionar o servidor vCenter ao Unified Manager. Isso é necessário para o polling de configuração.

Para cada vCenter Server adicionado e descoberto, o Unified Manager coleta os dados de configuração, como os detalhes do vCenter Server e do servidor ESXi, o mapeamento do ONTAP, os detalhes do datastore e o número de VMs hospedadas. Ele também coleta as métricas de desempenho dos componentes.

Passos

1. Acesse **VMWARE** > **vCenter**, e verifique se o seu vCenter Server está disponível na lista.

   Se o seu vCenter Server não estiver disponível, você precisará adicionar o vCenter Server.

   a. Clique em **Add**.
   b. Adicione o endereço IP correto para o servidor vCenter e certifique-se de que o dispositivo esteja acessível.
   c. Adicione o nome de usuário e a senha do administrador ou usuário raiz com acesso somente leitura ao vCenter Server.
   d. Adicione o número da porta personalizada se estiver usando uma porta diferente da porta padrão 443.
   e. Clique em **Salvar**.

      Após a detecção bem-sucedida, o sistema exibe um certificado do servidor para que você o aceite.

   Ao aceitar o certificado, o vCenter Server é adicionado à lista de vCenter Servers disponíveis. Adicionar o dispositivo não resulta em 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 o status dele passando o mouse sobre o campo **Status** para ver se o seu vCenter Server está funcionando como esperado ou se há algum aviso ou erro.

   Adicionar o servidor vCenter 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 servidor vCenter para serem refletidos com precisão.

   - Verde: "Normal", indicando que o vCenter Server foi descoberto e que as métricas de desempenho foram coletadas com sucesso
   - Amarelo: "Aviso" (por exemplo, quando o nível de estatísticas do servidor vCenter não foi definido como 3 ou superior para obter estatísticas de cada objeto)
   - Laranja: "erro" (indica quaisquer erros internos, como exceção, falha na coleta de dados de configuração ou o servidor vCenter estar inacessível) Você pode clicar no ícone de exibição da coluna ("Mostrar/Ocultar") para ver a mensagem de status de um servidor vCenter e solucionar o problema.

3. Caso o servidor vCenter esteja inacessível ou as credenciais tenham mudado, edite os detalhes do servidor vCenter selecionando **vCenter** > **Editar**.
4. Faça as alterações necessárias na página **Edit VMware vCenter Server**.
5. Clique em **Salvar**.

vCenter Server inicia a coleta de dados

vCenter Server coleta amostras de dados de desempenho em tempo real a cada 20 segundos e as consolida em amostras de 5 minutos. O agendamento da coleta de dados de desempenho do Unified Manager baseia-se 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 os discos virtuais, as VMs e os hosts. Para datastores, o Unified Manager calcula uma média horária de IOPS e latência com base em amostras obtidas do ONTAP. Esses valores ficam disponíveis no início de cada hora. As métricas de desempenho não ficam disponíveis imediatamente após a adição do vCenter Server e ficam disponíveis somente quando a próxima hora começa. A sondagem de dados de desempenho começa após a conclusão

de um ciclo de coleta de dados de configuração.

Para a coleta de dados de configuração do servidor vCenter, o Unified Manager segue a mesma programação da coleta de dados de configuração do cluster. Para obter informações sobre a programação da coleta de dados de configuração e desempenho do servidor vCenter, consulte "atividade de coleta de dados de configuração e desempenho do cluster".

Informações relacionadas

"Atividade de coleta de dados de configuração e desempenho do cluster"

Remover um vCenter Server do Active IQ Unified Manager

Você pode remover 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 nesse 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 de máquinas virtuais.

Antes de começar

Antes de remover os servidores vCenter, certifique-se do seguinte:

- Você possui a função de Administrador de Aplicativos ou a função de Administrador de Armazenamento.
- Você deve estar ciente dos nomes dos servidores vCenter e dos respectivos endereços IP associados a eles.

Passos

1. No painel de navegação à esquerda, clique em **VMWARE>vCenter**.
2. Na página vCenters, selecione o vCenter Server que você deseja remover e clique em **Remover**.
3. Na caixa de diálogo de mensagem **Remover vCenter**, clique em **OK** para confirmar a solicitação de remoção.

Entenda como o Active IQ Unified Manager monitora máquinas virtuais

Para qualquer problema de latência nas aplicações de máquina virtual (VM), talvez seja necessário monitorar as VMs para analisar e solucionar a causa. As VMs ficam disponíveis quando o servidor vCenter e os clusters ONTAP que hospedam o storage das VMs são adicionados ao Unified Manager.

Você vê os detalhes das VMs na página **VMWARE** > > **Virtual Machines**. São exibidas informações, como disponibilidade, status, capacidade usada e alocada, latência de rede e os IOPS e a latência da VM, do datastore e do host. Para uma VM compatível com vários datastores, a grade mostra as métricas do datastore com a pior latência, com um ícone de asterisco (*) indicando datastores adicionais. Se você clicar no ícone, as métricas do datastore adicional serão exibidas. Algumas dessas colunas não estão disponíveis para classificação e filtragem.



Para visualizar uma máquina virtual e seus detalhes, a descoberta (polling ou coleta de métricas) do cluster ONTAP deve estar concluída. Se o cluster for removido do Unified

Manager, a máquina virtual 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 datastore conectados a ela. A visualização da topologia exibe os componentes subjacentes em suas camadas específicas, na seguinte ordem: **disco virtual** > **VM** > **host** > **rede** > **datastore** > **VMDK**.

Você pode determinar o caminho de E/S e as latências em nível de componente a partir de uma perspectiva topológica e identificar se o storage é a causa do problema de desempenho. A visualização resumida da topologia exibe o caminho de E/S e destaca o componente que apresenta problemas de IOPS e latência para que você possa decidir as etapas de solução de problemas. Você também pode ter uma visualização expandida da topologia que mostra cada componente separadamente, juntamente com a latência desse componente. Você pode selecionar um componente para determinar o caminho de E/S destacado nas camadas.

Ver a topologia de resumo

Para identificar problemas de desempenho visualizando as VMs em uma topologia resumida:

1. Acesse **VMWARE** > **Virtual Machines**.
2. Procure sua máquina virtual digitando o nome dela na caixa de pesquisa. Você também pode filtrar os resultados da pesquisa com base em critérios específicos clicando no botão **Filtrar**. No entanto, se você não encontrar sua máquina virtual, verifique se o vCenter Server correspondente foi adicionado e descoberto.

> Os servidores vCenter permitem caracteres especiais, como %, &, *, $, #, @, !, \, /, :, *, ?, "`, <, >, |, ;, ', nos nomes de entidades do vSphere, como VM, cluster, datastore, pasta ou arquivo. O VMware vCenter Server e o ESX/ESXi Server não escapam caracteres especiais usados nos nomes de exibição. No entanto, quando o nome é processado no Unified Manager, ele é exibido de forma diferente. Por exemplo, uma VM chamada `%$VC_AIQUM_clone_191124%` no vCenter Server é exibida como `%25$VC_AIQUM_clone_191124%25` no Unified Manager. Você deve anotar esse problema ao consultar uma VM com um nome que contenha caracteres especiais.

3. Verifique o status da VM. Os status da VM são obtidos do vCenter Server. Os seguintes status estão disponíveis. Para obter mais informações sobre esses status, consulte a documentação da VMware.
   - Normal
   - Aviso
   - Alerta
   - Não monitorado
   - Desconhecido
4. Clique na seta para baixo ao lado da VM para ver a visualização resumida da topologia dos componentes nas camadas de computação, rede e storage. O nó que tem problemas de latência é destacado. A visualização resumida exibe a pior latência dos componentes. Por exemplo, se uma VM tiver mais de um disco virtual, essa visualização exibirá o disco virtual com a pior latência entre todos os discos virtuais.
5. Para analisar a latência e a taxa de transferência do datastore ao longo de um período, clique no botão **Workload Analyzer** acima do ícone do objeto do datastore. Você acessará a página Workload Analysis, onde poderá selecionar um intervalo de tempo e visualizar os gráficos de desempenho do datastore. Para obter mais informações sobre o workload analyzer, consulte *Solução de problemas de cargas de trabalho usando o workload analyzer*.

Ver topologia expandida

Você pode detalhar cada componente separadamente visualizando a topologia expandida da VM.

Passos

1. Na visualização resumida da topologia, clique em **Expand Topology**. Você pode ver a topologia detalhada de cada componente separadamente, com os números de latência de cada objeto. Se houver vários nós em uma categoria, por exemplo, vários nós no datastore ou no VMDK, o nó com a pior latência será destacado em vermelho.
2. Para verificar o caminho de E/S de um objeto específico, clique nesse objeto para visualizar o caminho de E/S e o mapeamento correspondente. Por exemplo, para visualizar o mapeamento de um disco virtual, clique no disco virtual para ver o mapeamento destacado para o respectivo VMDK. Em caso de lentidão no desempenho desses componentes, você pode coletar mais dados do ONTAP e solucionar o problema.

> As métricas não são exibidas para VMDKs. Na topologia, apenas os nomes dos VMDKs são mostrados, e não as métricas.

Informações relacionadas

"Solução de problemas de cargas de trabalho usando o workload Analyzer"

Visualize a infraestrutura virtual em um cenário de recuperação de desastres com o Active IQ Unified Manager

Você pode visualizar a configuração e as métricas de desempenho dos datastores hospedados em uma configuração do MetroCluster ou em uma configuração de recuperação de desastres da máquina virtual de storage (storage VM) (SVM DR).

No Unified Manager, você pode visualizar os volumes NAS ou LUNs em uma configuração do MetroCluster que estão anexados como datastores no vCenter Server. Os datastores hospedados em uma configuração do MetroCluster são representados na mesma visualização topológica que um datastore em um ambiente padrão.

Você também pode visualizar os volumes NAS ou LUNs em uma configuração de recuperação de desastres de VM de storage que estão mapeados para os datastores no vCenter Server.

Visualizar armazenamentos de dados na configuração do MetroCluster

Observe os seguintes pré-requisitos antes de visualizar os datastores em uma configuração do MetroCluster:

- Em caso de switchover e switchback, a descoberta dos clusters primário e secundário do par de HA e dos servidores vCenter deve estar concluída.
- Os clusters primário e secundário do par de 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 do ONTAP 9"

Siga estas etapas para visualizar os datastores:

1. Na página **VMWARE** > **Virtual Machines**, clique na VM que hospeda o datastore. Clique em **Workload**

Analyzer ou no link do objeto datastore. No cenário padrão, quando o site primário que hospeda o volume ou LUN está funcionando conforme o esperado, você pode ver os detalhes do cluster vServer do site primário.

2. Em caso de desastre e de um switchover consecutivo para o site secundário, o link do datastore aponta para as métricas de desempenho do volume ou LUN no cluster secundário. Isso se reflete após a conclusão do próximo ciclo de descoberta (aquisição) de clusters e vServer.
3. Após uma reversão bem-sucedida, o link do datastore volta a refletir as métricas de desempenho do volume ou LUN no cluster primário. Isso se reflete após a conclusão do próximo ciclo de descoberta de clusters e de vServer.

Visualizar datastores na configuração de recuperação de desastres da VM de storage

Observe os seguintes pré-requisitos antes de visualizar datastores em uma configuração de recuperação de desastres de VM de storage:

- Em caso de switchover e switchback, a descoberta dos clusters primário e secundário do par de HA e dos servidores vCenter deve estar concluída.
- Tanto os clusters de origem e de destino quanto os pares de VM de storage devem ser gerenciados pelo Unified Manager.
- A configuração necessária deve ser concluída no ONTAP e no vCenter Server.
    - Para datastores NAS (NFS e VMFS), em caso de desastre, as etapas incluem ativar a máquina virtual de storage secundário, verificar as LIFs de dados e as rotas, restabelecer as conexões perdidas no vCenter Server e iniciar as VMs.

      Para retornar ao site primário, os dados entre os volumes devem ser sincronizados antes que o site primário comece a fornecer os dados.

    - Para datastores SAN (iSCSI e FC para VMFS), o vCenter Server formata o LUN montado em formato VMFS. Em caso de desastre, as etapas incluem ativar a VM de storage secundário, verificar as LIFs de dados e as rotas. Se os IPs do destino iSCSI forem diferentes dos das LIFs primárias, será necessário adicioná-los manualmente. Os novos LUNs devem estar disponíveis como dispositivos no adaptador iSCSI do adaptador de storage do host. Depois disso, você deve criar novos datastores VMFS com os novos LUNs e registrar as VMs antigas com novos nomes. As VMs devem estar 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 devem ser registradas com novos nomes.

      Para obter informações sobre a configuração, consulte a documentação do ONTAP e do vCenter Server.

  "Centro de Documentação do ONTAP 9"

Siga estas etapas para visualizar os datastores:

1. Na página **VMWARE** > **Virtual Machines**, clique no inventário da VM que hospeda o datastore. Clique no link do objeto do datastore. No cenário padrão, você pode ver os dados de desempenho dos volumes e LUNs na VM de storage primário.
2. Em caso de desastre e de um switchover consecutivo para a VM de storage secundário, o link do datastore aponta para as métricas de desempenho do volume ou LUN na VM de storage secundário. Isso se reflete após a conclusão do próximo ciclo de descoberta (aquisição) de clusters e vServer.

3. Após um switchback bem-sucedido, o link do datastore volta a refletir as métricas de desempenho do volume ou da LUN na VM de storage primário. Isso é refletido após a conclusão do próximo ciclo de descoberta de clusters e de vServer.

Cenários não suportados

- Para uma configuração do MetroCluster, observe as seguintes limitações:
  - Apenas os clusters nos estados `NORMAL` e `SWITCHOVER` são considerados. Outros estados, como `PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK` e `NOT_REACHABLE`, não são suportados.
  - A menos que o Automatic Switch Over (ASO) esteja habilitado, se o cluster primário ficar inativo, o cluster secundário não poderá ser detectado, e a topologia continuará apontando para o volume ou LUN no cluster primário.
- Para uma configuração de recuperação de desastres de VM de storage, observe a seguinte limitação:
  - Não há suporte para uma configuração com o Site Recovery Manager (SRM) ou o Storage Replication Adapter (SRA) habilitados para um ambiente de storage SAN.

Provisionar e gerenciar cargas de trabalho

Provisione e gerencie cargas de trabalho no Active IQ Unified Manager

O recurso de gerenciamento do Active IQ Unified Manager fornece Performance Service Levels, Storage Efficiency Policies e APIs de provedores de storage para provisionamento, monitoramento e gerenciamento de workloads de storage em um data center.

O Unified Manager fornece essa funcionalidade por padrão. Você pode desativá-la em **Gerenciamento de storage** > **Configurações de recursos** caso não pretenda utilizá-la.

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 storage, às cargas de trabalho e gerenciar seu ambiente de storage com base nessas políticas.

Este recurso permite as seguintes funções:

- Descoberta automática de cargas de trabalho de storage nos clusters adicionados, permitindo avaliação e implantação fáceis das cargas de trabalho de storage
- Provisionamento de cargas de trabalho NAS compatíveis com os protocolos NFS e CIFS
- Provisionamento de cargas de trabalho SAN com suporte aos protocolos iSCSI e FCP
- Suporte para os protocolos NFS e CIFS no mesmo compartilhamento de arquivos
- Gerenciamento dos níveis de serviço de desempenho e das políticas de eficiência de storage
- Atribuição de níveis de serviço de desempenho e políticas de eficiência de armazenamento a cargas de trabalho de armazenamento

As opções **Provisioning**, **Storage** > **Workloads** e **Policies** no painel esquerdo da interface de usuário permitem que você modifique várias configurações.

Você pode executar as seguintes funções usando estas opções:

- Visualize as cargas de trabalho de storage na página **Storage** > **Workloads**
- Crie cargas de trabalho de armazenamento a partir da página Provision Workload
- Criar e gerenciar níveis de serviço de desempenho a partir de políticas
- Criar e gerenciar políticas de eficiência de storage em Policies
- Atribua políticas às cargas de trabalho de storage na página Workloads

Informações relacionadas

"Gerenciamento de storage baseado em políticas"

Visão geral das cargas de trabalho

Saiba mais sobre o painel de cargas de trabalho no Active IQ Unified Manager

Uma carga de trabalho representa as operações de entrada/saída (E/S) de um objeto de storage, como um volume ou LUN. A forma como o storage é provisionado se baseia nos requisitos esperados da carga de trabalho. As estatísticas da carga de trabalho são rastreadas pelo Active IQ Unified Manager somente depois que há tráfego de entrada e saída no objeto de storage. 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 um aplicativo de e-mail.

A página Workloads exibe um resumo das cargas de trabalho de storage dos clusters ONTAP gerenciados pelo Unified Manager. Ela fornece informações cumulativas e resumidas sobre as cargas de trabalho de storage que estão em conformidade com o Performance Service Level, bem como sobre as cargas de trabalho de storage que não estão em conformidade. Ela também permite avaliar a capacidade total, disponível e usada, além do desempenho (IOPS) dos clusters em todo o seu data center.

Recomenda-se que você avalie o número de cargas de trabalho de armazenamento que não estão em conformidade, estão indisponíveis ou não são gerenciadas por nenhum Performance Service Level e tome as medidas necessárias para garantir sua conformidade, uso de capacidade e IOPS.

A página Workloads possui 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 do ONTAP gerenciados pelo Unified Manager.
- Visão geral do data center: fornece uma visão geral da capacidade e das IOPS das cargas de trabalho de storage no data center. Os dados relevantes são exibidos no nível do data center e para cada .

Seção de visão geral das cargas de trabalho

A seção de visão geral das cargas de trabalho fornece informações cumulativas e resumidas 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 às quais os Níveis de Serviço de Desempenho foram atribuídos:
  - **Em conformidade**: o desempenho das cargas de trabalho de armazenamento se baseia nos Níveis de Serviço de Desempenho atribuídos a elas. Se as cargas de trabalho de armazenamento estiverem

dentro do limite de latência definido 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 storage são marcadas como “não conformes” se a latência das cargas de trabalho de storage exceder o limite de latência definido no Nível de Serviço de Desempenho associado. As cargas de trabalho não conformes são marcadas em laranja.
    - **Indisponível**: As cargas de trabalho de storage são marcadas como “unavailable” se estiverem offline ou se o cluster correspondente estiver inacessível. As cargas de trabalho indisponíveis são marcadas em vermelho.
- **Não atribuído**: as cargas de trabalho de storage que não têm um Nível de Serviço de Desempenho atribuído aparecem como “não atribuído”. O número é indicado pelo ícone de informação.

A contagem total de cargas de trabalho é a soma 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 Workloads.

A subseção Conformidade por Níveis de Serviço de Desempenho exibe o número total de cargas de trabalho de armazenamento disponíveis:

- Em conformidade com cada tipo de Nível de Serviço de Desempenho
- Para os quais existe uma discrepância entre os níveis de serviço de desempenho atribuídos e os recomendados

Seção de visão geral do data center

A seção de visão geral do data center representa graficamente a capacidade disponível e utilizada, bem como as IOPS de todos os clusters no data center. Com esses dados, você deve gerenciar a capacidade e as IOPS das cargas de trabalho de storage. A seção também exibe as seguintes informações para as cargas de trabalho de storage em todos os clusters:

- A capacidade total, disponível e utilizada de todos os clusters em seu data center
- Os IOPS totais, disponíveis e usados de todos os clusters no seu data center
- A capacidade disponível e utilizada com base em cada Nível de Serviço de Desempenho
- As IOPS disponíveis e usadas com base em cada Nível de Serviço de Desempenho
- O espaço total e as IOPS usadas pelas cargas de trabalho que não têm Performance Service Level atribuído

Como a capacidade e o desempenho do data center são calculados com base nos Níveis de Serviço de Desempenho

A capacidade utilizada e as IOPS são obtidas com base na capacidade total utilizada e no desempenho de todas as cargas de trabalho de storage nos clusters.

O IOPS disponível é calculado com base na latência esperada e nos Níveis de Serviço de Desempenho (PSL) recomendados nos nós. Inclui o IOPS disponível para todos os PSL cuja latência esperada seja 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 nos agregados. Ela inclui a capacidade disponível para todos os níveis de serviço de desempenho cuja latência esperada seja menor ou igual à própria latência esperada.

Visualize as cargas de trabalho no Active IQ Unified Manager

Ao adicionar clusters ao Unified Manager, as cargas de trabalho de armazenamento em cada cluster são descobertas e exibidas automaticamente na página Workloads.

O Unified Manager começa a analisar as cargas de trabalho para recomendação (PSLs recomendados) somente após o início das operações de E/S nas cargas de trabalho de armazenamento.

Os volumes de FlexGroup e seus constituintes estão 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, bem como a visão geral do espaço e do 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 distribuição da contagem de cargas de trabalho para cada PSL também é exibida. Clicar nas contagens leva você à 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 **Data Center Overview**: exibe o espaço disponível e usado (TiB) e o desempenho (IOPS) do data center. Também é exibida uma discriminação do espaço disponível e usado (TiB) e do desempenho (IOPS) de todas as cargas de trabalho em cada PSL.

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 do 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 “Waiting for I/O”. Após o início das operações de E/S nas cargas de trabalho de armazenamento, o Unified Manager inicia a análise e o status da carga de trabalho muda para “Learning…”. Após a conclusão da análise (dentro de 24 horas a partir do início das operações de E/S), os PSLs recomendados são exibidos para as cargas de trabalho de armazenamento.

A página também permite atribuir Políticas de Eficiência de Armazenamento (SEPs) e Níveis de Serviço de Desempenho (PSLs) às cargas de trabalho de armazenamento. Você pode executar várias tarefas:

- Adicionar ou provisionar cargas de trabalho de armazenamento
- Visualize e filtre a lista de cargas de trabalho
- Atribua PSLs às cargas de trabalho de armazenamento
- Avalie os PSLs recomendados pelo sistema e atribua-os às cargas de trabalho
- Atribua SEPs às cargas de trabalho de armazenamento

Adicionar ou provisionar cargas de trabalho de armazenamento

Você pode adicionar ou provisionar as cargas de trabalho de armazenamento para LUNs compatíveis (com suporte aos 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".

Visualizando e filtrando 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 por cluster de host ou VM de armazenamento. A opção **Capacidade Total** permite filtrar pela capacidade total das cargas de trabalho (em MB). No entanto, nesse caso, o número de cargas de trabalho retornadas pode variar, pois a capacidade total é comparada em nível de byte.

Para cada carga de trabalho, são exibidas informações, como o cluster de hosts e a máquina virtual de armazenamento, 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 as IOPS, a capacidade e a latência da carga de trabalho clicando no botão **Escolher / Ordenar Colunas** e selecionando colunas específicas para visualizar. A coluna Performance View exibe a média e o pico de IOPS de uma carga de trabalho, e você pode clicar no ícone do analisador de carga de trabalho para visualizar a análise detalhada de IOPS.

Analisar os critérios de desempenho e capacidade de uma carga de trabalho

O botão **Analisar Carga de Trabalho** na janela pop-up **Análise de IOPS** leva você à 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 da 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".

Para visualizar informações de desempenho sobre uma carga de trabalho e ajudar na solução de problemas, clique no ícone de gráfico de barras na coluna **Visualização de desempenho**. Para visualizar gráficos de desempenho e capacidade na página Análise da carga de trabalho e analisar o objeto, clique no botão **Analisar carga de trabalho**.

Para obter mais informações, consulte "Que dados o analisador de carga de trabalho exibe".

Atribua políticas às cargas de trabalho no Active IQ Unified Manager

Você pode atribuir Políticas de Eficiência de Armazenamento (SEPs) e Níveis de Serviço de Desempenho (PSLs) às cargas de trabalho de armazenamento na página All Workloads, usando as diferentes opções de navegação.

Atribua 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 necessário, ou ambos.

4. Clique no ícone de marca de seleção para aplicar as alterações.

> Você também pode selecionar uma carga de trabalho e clicar em **More Actions** para atribuir as políticas.

Atribua políticas a várias cargas de trabalho de armazenamento

Você pode atribuir um PSL ou um SEP a várias cargas de trabalho de armazenamento simultaneamente. Siga estes passos:

1. Selecione 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 uma SEP, selecione **Atribuir Política de Eficiência de Armazenamento**. Uma janela pop-up é exibida para você selecionar a política.
4. Selecione a política apropriada e clique em **Aplicar**. O número de cargas de trabalho às quais as políticas estão atribuídas é exibido. As cargas de trabalho às quais as políticas não estão atribuídas também são listadas, juntamente com a causa.

> A aplicação de políticas em lote em cargas de trabalho pode levar algum tempo, dependendo da quantidade 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 lote for concluída, você poderá visualizar o status de conclusão. Se você estiver aplicando uma PSL em várias cargas de trabalho, não poderá acionar outra solicitação enquanto a tarefa anterior de atribuição em lote estiver em execução.

Atribua PSLs recomendadas pelo sistema às cargas de trabalho

Você pode atribuir PSLs recomendadas pelo sistema às cargas de trabalho de armazenamento em um data center que não têm PSLs atribuídas ou cujas PSLs atribuídas não correspondem à recomendação do sistema. Para usar essa funcionalidade, clique no botão **Atribuir PSLs recomendadas pelo sistema**. Não é necessário selecionar cargas de trabalho específicas.

A recomendação é determinada internamente pela análise do sistema e é ignorada para cargas de trabalho cujos IOPS e outros parâmetros não coincidem com as definições de qualquer PSL disponível. Cargas de trabalho de armazenamento com status de `Waiting for I/O` e de aprendizado também são excluídas.

> Existem 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 PSL **Extreme Performance** é recomendado. E quando a carga de trabalho tem as letras “vm” no nome, o PSL **Performance** é recomendado.

Veja também o artigo da base de conhecimento (KB) "O ActiveIQ Unified Manager "Assign System Recommended Performance Service Level" não é adaptável a uma carga de trabalho altamente variável"

Provisione volumes de compartilhamento de arquivos no Active IQ Unified Manager

Você pode criar volumes de compartilhamento de arquivos que oferecem suporte aos

protocolos CIFS/SMB e NFS em um cluster existente e em uma máquina virtual de storage (storage VM) na página Provision Workload.

Antes de começar

- A VM de storage deve ter espaço para provisionar o volume de compartilhamento de arquivos.
- Um ou ambos os serviços SMB e NFS devem estar habilitados na sua máquina virtual de storage.
- Para selecionar e atribuir o Nível de Serviço de Desempenho (PSL) e a Política de Eficiência de Storage (SEP) à 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, em seguida, selecione o cluster na lista disponível.
2. Com base no cluster que você selecionou, o campo **VM de storage** filtra as VMs de storage disponíveis para esse cluster. Selecione a VM de storage necessária na lista.

   Com base nos serviços SMB e NFS compatíveis na máquina virtual de storage, a opção NAS é ativada na seção Informações do host.

3. Na seção Armazenamento e Otimização, atribua a capacidade de storage e o PSL e, opcionalmente, um SEP para a carga de trabalho.

   As especificações do SEP são atribuídas ao LUN e as definições do PSL são aplicadas à carga de trabalho quando ela é criada.

4. Selecione a caixa de seleção **Impor limites de desempenho** se você quiser impor o PSL que 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 suportar os objetivos de desempenho e capacidade definidos na respectiva política. Por exemplo, se uma carga de trabalho tiver o PSL "Extreme Performance" atribuído, o agregado no qual a carga de trabalho será provisionada deverá ter a capacidade de suportar os objetivos de desempenho e capacidade da política "Extreme Performance", como armazenamento SSD.

   > A menos que você selecione esta caixa de seleção, o PSL não se aplica à carga de trabalho, e o status da carga de trabalho no painel aparece como não atribuída.

5. Selecione a opção **NAS**.

   Se você não vir a opção **NAS** habilitada, verifique se a VM de storage selecionada oferece suporte a SMB ou NFS, ou a ambos.

   > Se a sua máquina virtual de storage estiver habilitada para os serviços SMB e NFS, você poderá selecionar as caixas de seleção **Share by NFS** e **Share by SMB** e criar um compartilhamento de arquivos que ofereça suporte aos protocolos NFS e SMB. Se você quiser criar um compartilhamento SMB ou CIFS, selecione apenas a respectiva caixa de seleção.

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 vírgula 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 storage, e a política de exportação para esse host é criada ou, caso já exista uma política, ela é reutilizada. Se vários compartilhamentos NFS forem criados para o mesmo host, uma política de exportação disponível para esse host com regras correspondentes será reutilizada para todos os compartilhamentos de arquivos. A função de especificar regras de políticas individuais ou reutilizar políticas fornecendo chaves de política específicas está disponível quando você provisiona o compartilhamento NFS usando APIs.

7. Para um compartilhamento SMB, especifique quais usuários ou grupos de usuários podem acessar o compartilhamento SMB e 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 storage.

Provisionar LUNs no Active IQ Unified Manager

Você pode criar LUNs que oferecem suporte aos protocolos CIFS/SMB e NFS em um cluster existente e em uma Storage Virtual Machine (storage VM) existente na página Provision Workload.

Antes de começar

- A máquina virtual de storage deve ter espaço para provisionar o LUN.
- Tanto o iSCSI quanto o FCP devem estar habilitados na máquina virtual 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 Storage (SEP) à 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, em seguida, selecione o cluster na lista disponível.

   Com base no cluster que você selecionou, o campo **VM de armazenamento** filtra as VMs de armazenamento disponíveis para esse cluster.

2. Selecione na lista a máquina virtual de armazenamento que oferece suporte aos serviços iSCSI e FCP.

   Com base na sua seleção, a opção SAN é ativada na seção Host Information.

3. Na seção **Armazenamento e Otimização**, atribua a capacidade de storage e o PSL e, opcionalmente, o SEP para a carga de trabalho.

   As especificações do SEP são atribuídas ao LUN e as definições do PSL são aplicadas à carga de trabalho quando ela é criada.

4. Selecione a caixa de seleção **Impor limites de desempenho** se você quiser 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 suportar os objetivos de desempenho e capacidade definidos na respectiva política. Por exemplo, se uma carga de trabalho receber o PSL "Extreme Performance", o agregado no qual a carga de trabalho

será provisionada deverá ter a capacidade de suportar os objetivos de desempenho e capacidade da política "Extreme Performance", como storage 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 storage que você selecionou é compatível com iSCSI e FCP.
6. Selecione o sistema operacional do host.
7. Especifique o mapeamento de host para controlar o acesso dos iniciadores ao LUN. Você pode atribuir grupos de iniciadores (igroups) existentes ou definir e mapear novos igroups.

> Se você criar um novo igroup durante o provisionamento do LUN, precisará aguardar o próximo ciclo de descoberta (até 15 minutos) para usá-lo. Portanto, é recomendável que você use um igroup existente na lista de igroups disponíveis.

   Se você quiser criar um novo igroup, selecione o botão **Criar um novo grupo de iniciadores** e insira as informações do igroup.

8. Clique em **Salvar**.

   A LUN é adicionada à lista de workloads de storage.

Gerenciar os níveis de serviço de desempenho

Gerencie os níveis de serviço de desempenho no Active IQ Unified Manager

Um Nível de Serviço de Desempenho (PSL) permite definir os objetivos de desempenho e storage 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 de recursos de storage são baseados em Objetivos de Nível de Serviço (SLOs). Os SLOs são definidos por contratos de nível de serviço baseados no desempenho e na capacidade necessários. No Unified Manager, os SLOs referem-se às definições de PSL dos aplicativos que estão em execução no storage NetApp. Os serviços de storage são diferenciados com base no desempenho e na utilização dos recursos subjacentes. Um PSL é uma descrição dos objetivos do serviço de storage. Um PSL permite que o provedor de storage especifique os objetivos de desempenho e capacidade para a carga de trabalho. Quando você atribui um PSL a uma carga de trabalho, a carga de trabalho correspondente no ONTAP é gerenciada por seus objetivos de desempenho e capacidade. Cada PSL é regido por IOPs de pico, esperados e mínimos absolutos, além da latência esperada.

O Unified Manager possui os seguintes tipos de PSLs:

- **Definido pelo sistema**: o Unified Manager fornece algumas políticas predefinidas que não podem ser alteradas. Essas PSLs predefinidas são:
  - Desempenho Extremo
  - Desempenho
  - Valor

    Os PSLs Extreme Performance, Performance e Value são aplicáveis à maioria das cargas de trabalho

de storage comuns em um data center.

O Unified Manager também oferece três Níveis de Serviço de Desempenho (PSLs) para aplicações de banco de dados. Esses PSLs são de altíssimo desempenho, suportam picos de IOPS e são adequados para aplicações de banco de dados com a maior demanda de throughput.

  - Extreme 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 Níveis de Serviço de Desempenho para atendê-las. Para obter mais informações, consulte "Criar e editar Níveis de Serviço de Desempenho".
- **Beyond Extreme**: os PSLs Beyond Extreme são os PSLs recomendados pelo sistema para cargas de trabalho que exigem IOPS superiores ao Extreme. As cargas de trabalho são analisadas internamente com base em seus IOPS, capacidade e latência, e um PSL Beyond Extreme é recomendado para cada uma dessas cargas de trabalho na tela **Storage > Workloads > All Workloads**. Você pode aplicar os PSLs às cargas de trabalho para garantir o desempenho ideal.

  Os parâmetros de IOPs para as cargas de trabalho são gerados dinamicamente, dependendo do comportamento da carga de trabalho, e anexados ao nome do PSL Beyond Extreme no formato `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`. Por exemplo, se o sistema determinar que uma carga de trabalho tem os IOPs de pico e esperados como `106345` e `37929`, respectivamente, o PSL Beyond Extreme gerado para a carga de trabalho é nomeado como `Beyond Extreme 106345 37929`. Embora esses PSLs sejam recomendados pelo sistema, quando você os atribui às cargas de trabalho, esses PSLs são rotulados como `User-defined` em tipo.

Gerencie as 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 individualmente. Quaisquer modificações também podem ser gerenciadas reatribuindo outro PSL, em vez de gerenciá-las individualmente. O Unified Manager ajuda você a atribuir PSLs às suas cargas de trabalho com base em avaliação e recomendações internas.

Para obter informações sobre como atribuir PSLs recomendados pelo sistema às cargas de trabalho, consulte "Atribua PSLs recomendadas pelo sistema às cargas de trabalho"

A página de Níveis de Serviço de Desempenho lista as políticas de PSL disponíveis e permite adicioná-las, editá-las e excluí-las.

> Não é possível modificar um PSL que seja definido pelo sistema ou que esteja atualmente atribuído a uma carga de trabalho. Também não é possível excluir um PSL que esteja atribuído a uma carga de trabalho ou que seja o único PSL disponível.

Esta página exibe as seguintes informações:

Campo	Descrição
Nome	Nome da PSL.
Tipo	Se a política é definida pelo sistema ou pelo usuário.

Campo	Descrição
IOPS/TB esperados	Número mínimo de IOPS que se espera que um aplicativo execute em uma LUN ou compartilhamento de arquivos. O valor de IOPS esperado especifica o mínimo de IOPS alocados, com base no tamanho alocado do objeto de armazenamento.
Pico de IOPS/TB	Número máximo de IOPS que um aplicativo pode executar em um LUN ou compartilhamento de arquivos. O IOPS de pico especifica o máximo de IOPS possível alocado, com base no tamanho alocado ou no tamanho usado do objeto de armazenamento. O pico de IOPS é baseado 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 storage. 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 storage, levando em conta as eficiências de storage. Por padrão, a política de alocação é definida como espaço usado.

Campo	Descrição
IOPS mínimos absolutos	O valor mínimo absoluto de IOPS é usado como substituição quando o IOPS esperado é inferior a esse valor. Os valores padrão dos PSLs definidos pelo sistema são os seguintes: • Desempenho extremo: se o IOPS esperado for >= 6144/TB, então o IOPS mínimo absoluto = 1000 • Desempenho: se o número esperado de IOPS for >= 2048/TB e < 6144/TB, então o número mínimo absoluto de IOPS será 500 • Valor: se o IOPS esperado for >= 128/TB e < 2048/TB, então o IOPS mínimo absoluto = 75 Os valores padrão dos PSLs de banco de dados definidos pelo sistema são os seguintes: • Extremo para logs de banco de dados: se o IOPS esperado for >= 22528, então o IOPS mínimo absoluto = 4000 • Extremo para dados compartilhados de banco de dados: se o IOPS esperado for maior ou igual a 16384, então o IOPS mínimo absoluto será igual a 2000 • Extremo para dados de banco de dados: se o IOPS esperado for maior ou igual a 12288, então o IOPS mínimo absoluto = 2000 O valor mais alto do IOPS mínimo absoluto para PSLs personalizados pode ser no máximo 75000. O valor mais baixo é calculado da seguinte forma: 1000/latência esperada
Latência esperada	Latência esperada para IOPS de storage em milissegundos por operação (ms/op).
Capacidade	Capacidade total disponível e utilizada nos clusters.
Cargas de trabalho	Número de cargas de trabalho de storage 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 do ONTAP, consulte o seguinte artigo da base de conhecimento: "O que é orçamento de desempenho?"

Eventos gerados para cargas de trabalho que ultrapassam 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 notificar você sobre um possível problema de desempenho:

- Limite de latência do volume da carga de trabalho excedido conforme definido pela Política de Nível de Serviço de Desempenho
- A latência da LUN da carga de trabalho ultrapassou o limite definido pela política de nível de serviço de desempenho.

Você pode querer analisar a carga de trabalho para ver o que pode estar causando os valores de latência mais altos.

Para obter mais informações, consulte os seguintes links:

- "Eventos de volume"
- "O que acontece quando uma política de limite de desempenho é violada"
- "Como o Unified Manager usa a latência 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)	Pico de IOPS	IOPS esperado	IOPS mínimos absolutos
Desempenho Extremo	Oferece altíssima taxa de transferência com latência muito baixa Ideal para aplicações sensíveis à latência	1	12288	6144	1000
Desempenho	Oferece alta taxa de transferência com baixa latência Ideal para aplicações de banco de dados e virtualizadas	2	4096	2048	500

Nível de serviço de desempenho	Descrição e caso de uso	Latência esperada (ms/op)	Pico de IOPS	IOPS esperado	IOPS mínimos absolutos
Valor	Oferece alta capacidade de storage e latência moderada Ideal para aplicações de alta capacidade, como e-mail, conteúdo web, compartilhamentos de arquivos e destinos de backup	17	512	128	75
Extreme para logs de banco de dados	Proporciona a taxa de transferência máxima com a menor latência. Ideal para aplicações de banco de dados que suportam logs de banco de dados. Este PSL oferece a maior taxa de transferência, pois os logs de banco de dados têm picos extremos e o registro em log é constantemente exigido.	1	45056	22528	4000

Nível de serviço de desempenho	Descrição e caso de uso	Latência esperada (ms/op)	Pico de IOPS	IOPS esperado	IOPS mínimos absolutos
Extremo para dados compartilhados de banco de dados	Proporciona altíssima taxa de transferência com a menor latência. Ideal para dados de aplicações de banco de dados armazenados em um armazenamento de dados comum, mas compartilhados entre bancos de dados.	1	32768	16384	2000
Extremo para dados de banco de dados	Oferece alta taxa de transferência com a menor latência. Ideal para dados de aplicações de banco de dados, como informações de tabelas de banco de dados e metadados.	1	24576	12288	2000

Crie e edite Níveis de Serviço de Desempenho no Active IQ Unified Manager

Quando os Níveis de Serviço de Desempenho definidos pelo sistema não corresponderem aos requisitos da sua carga de trabalho, você poderá criar seus próprios Níveis de Serviço de Desempenho otimizados para suas cargas de trabalho.

Antes de começar

- Você precisa ter a função de Application Administrator.
- O nome do Nível de Serviço de Desempenho deve ser único e você não pode usar as seguintes palavras-chave reservadas:

  `Prime`, `Extreme`, `Performance`, `Value`, `Unassigned`, `Learning`, `Idle`, `Default`, e `None`.

Você pode criar e editar 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, conforme você queira criar um novo Nível de Serviço de Desempenho ou editar um existente.

Para…	Siga estes passos…
Criar um novo nível de serviço de desempenho	Clique em **Add**.
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, em seguida, clique em **Submit** para salvar o nível de serviço de desempenho.

Você pode aplicar o novo ou alterado Performance Service Level às cargas de trabalho (LUNs, compartilhamentos de arquivos NFS, compartilhamentos CIFS) na página Workloads ou ao provisionar uma nova carga de trabalho.

Gerenciar políticas de eficiência de storage

Gerencie as políticas de eficiência de armazenamento no Active IQ Unified Manager

Uma Política de Eficiência de Storage (SEP, na sigla em inglês) permite que você defina as características de eficiência de storage de uma carga de trabalho. Você pode atribuir uma SEP a uma carga de trabalho ao criá-la inicialmente ou, depois, editando-a.

A eficiência de storage inclui o uso de tecnologias, como thin provisioning, deduplicação e compressão de dados, que aumentam a utilização do storage e reduzem os custos de storage. Ao criar SEPs, você pode usar essas tecnologias de economia de espaço individualmente ou em conjunto para alcançar a máxima eficiência de storage. Quando você associa as políticas às suas cargas de trabalho de storage, as configurações de política especificadas são atribuídas a elas. O Unified Manager permite atribuir SEPs definidas pelo sistema e pelo usuário para otimizar os recursos de storage 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 storage em um data center, no entanto, você pode criar suas próprias políticas se os SEPs definidos pelo sistema não atenderem aos seus requisitos.

Não é possível modificar um SEP que seja definido pelo sistema ou que esteja atualmente atribuído a uma carga de trabalho. Também não é possível excluir um SEP que esteja atribuído a uma carga de trabalho ou que seja o único SEP disponível.

A página Políticas de eficiência de storage lista as SEPs disponíveis e permite adicionar, editar e excluir SEPs personalizadas. Esta página exibe as seguintes informações:

Campo	Descrição
Nome	Nome da SEP.
Tipo	Se a política é definida pelo sistema ou pelo usuário.
Reserva de espaço	Se o volume é com thin provisioning ou com provisionamento espesso.
Desduplicação	Se a deduplicação está habilitada na carga de trabalho: • Inline: a desduplicação ocorre durante a gravação na carga de trabalho • Contexto: a desduplicação ocorre na carga de trabalho • Desativar: a deduplicação está desativada na carga de trabalho
Compressão	Se a compressão de dados está ativada na carga de trabalho: • Inline: a compressão de dados ocorre durante a gravação na carga de trabalho • Contexto: a compressão de dados ocorre na carga de trabalho • Desativar: a compressão de dados está desativada na carga de trabalho
Cargas de trabalho	Número de cargas de trabalho de storage às quais foi atribuído o SEP

Diretrizes para criar uma política personalizada de eficiência de storage

Se as SEPs existentes não atenderem aos requisitos de política para suas cargas de trabalho de armazenamento, você poderá criar uma SEP personalizada. No entanto, é recomendável que você tente usar as SEPs definidas pelo sistema para suas cargas de trabalho de armazenamento e crie SEPs personalizadas somente se necessário.

Você pode visualizar o SEP atribuído às cargas de trabalho na página All Workloads e na página de detalhes de Volume / Health. Você pode visualizar a taxa de redução de dados em nível de cluster, sem cópias Snapshot, com base nessas eficiências de storage no painel Capacity no Dashboard e na visualização Capacity: All Clusters.

Crie e edite políticas de eficiência de armazenamento no Active IQ Unified Manager

Quando as Políticas de Eficiência de Storage definidas pelo sistema não corresponderem aos requisitos da sua carga de trabalho, você poderá criar suas próprias Políticas de Eficiência de Storage otimizadas para suas cargas de trabalho.

Antes de começar

- Você precisa ter a função de Application Administrator.
- O nome da Política de Eficiência de Storage deve ser único, e você não pode usar as seguintes palavras-chave reservadas:

`High`, `Low`, `Unassigned`, `Learning`, `Idle`, `Default`, e `None`.

Você cria e edita Políticas de Eficiência de Storage personalizadas na página Políticas de Eficiência de Storage, definindo as características de eficiência de storage necessárias para os aplicativos que acessarão o storage.

Não é possível modificar uma política de eficiência de storage se ela estiver atribuída a uma carga de trabalho.

Passos

1. No painel de navegação esquerdo, em **Configurações**, selecione **Políticas** > **Eficiência de storage**.
2. Na página **Políticas de eficiência de storage**, clique no botão apropriado, dependendo de você querer criar uma nova Política de eficiência de storage ou editar uma Política de eficiência de storage existente.

Para…	Siga estes passos…
Criar uma nova Política de eficiência de storage	Clique em **Adicionar**
Editar uma política de eficiência de storage existente	Selecione uma política de eficiência de storage existente e clique em **Editar**

   A página para adicionar ou editar uma política de eficiência de storage é exibida.

3. Personalize a Política de eficiência de storage especificando as características de eficiência de storage e, em seguida, clique em **Enviar** para salvar a Política de eficiência de storage.

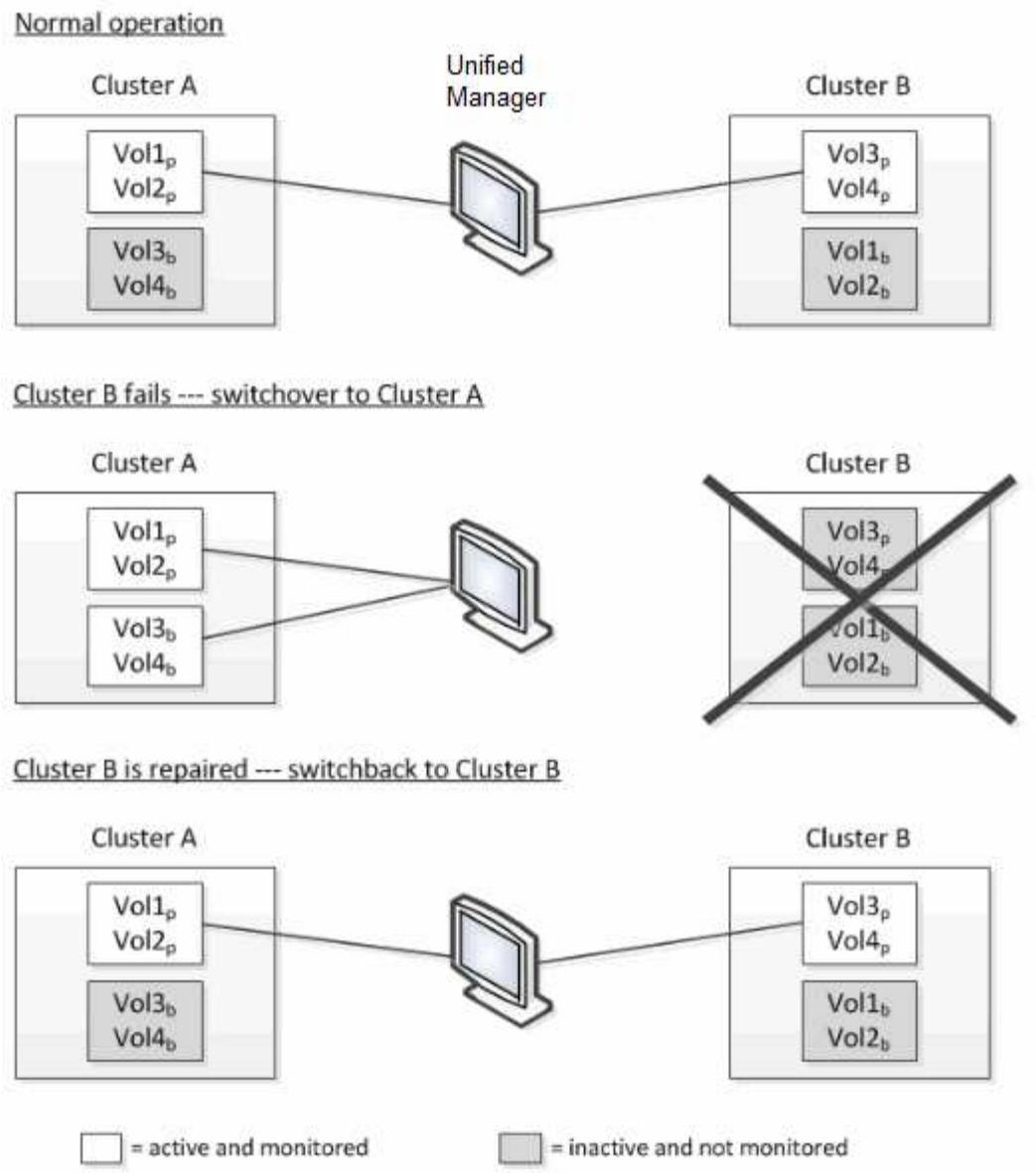
Você pode aplicar a Política de eficiência de storage nova ou alterada às cargas de trabalho (LUNs, compartilhamentos de arquivos NFS, compartilhamentos CIFS) na página Workloads ou ao provisionar uma nova carga de trabalho.

Gerencie e monitore as configurações do MetroCluster

Saiba mais sobre o comportamento do volume durante o switchover e o switchback no Active IQ Unified Manager

Eventos que acionam um switchover ou switchback fazem com que os volumes ativos sejam movidos de um cluster para o 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, recomenda-se monitorar ambos os clusters. Uma única instância do Unified Manager pode monitorar ambos os clusters em uma configuração do MetroCluster, mas, às vezes, a distância entre os dois locais exige o uso de duas instâncias do Unified Manager para monitorar ambos os clusters. A figura a seguir mostra uma única instância do Unified Manager:



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 por SnapMirror.

Durante o funcionamento normal:

- O Cluster A possui dois volumes ativos: Vol1p e Vol2p.
- O Cluster B possui dois volumes ativos: Vol3p e Vol4p.
- O Cluster A possui dois volumes inativos: Vol3b e Vol4b.
- O Cluster B possui dois volumes inativos: Vol1b e Vol2b.

O Unified Manager coleta informações referentes a cada um dos volumes ativos (estatísticas, eventos e assim por diante). As estatísticas de Vol1p e Vol2p são coletadas pelo Cluster A, e as estatísticas de Vol3p e Vol4p são coletadas pelo Cluster B.

Após uma falha catastrófica causar um switchover dos volumes ativos do Cluster B para o Cluster A:

- O Cluster A possui quatro volumes ativos: Vol1p, Vol2p, Vol3b e Vol4b.

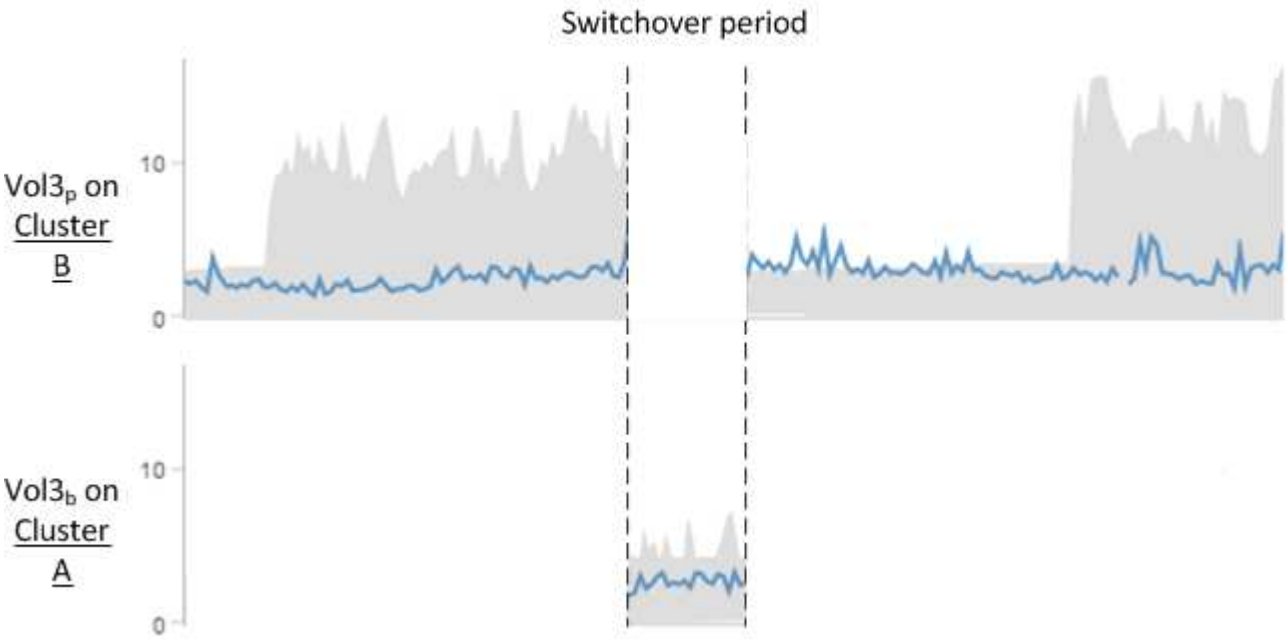
- O Cluster B possui quatro volumes inativos: Vol3p, Vol4p, Vol1b e Vol2b.

Assim como durante a operação normal, as informações referentes a cada um dos volumes ativos são coletadas pelo Unified Manager. Mas, neste caso, as estatísticas de Vol1p e Vol2p são coletadas pelo Cluster A, e as estatísticas de Vol3b e Vol4b também são coletadas pelo Cluster A.

Observe que Vol3p e Vol3b não são os mesmos volumes, pois estão em clusters diferentes. As informações no Unified Manager para Vol3p não são as mesmas que para Vol3b:

- Durante o switchover para o Cluster A, as estatísticas e os eventos do Vol3p não ficam visíveis.
- No primeiro switchover, o Vol3b aparece como um volume novo, sem nenhuma informação histórica.

Quando o Cluster B for reparado e um switchback for realizado, o Vol3p ficará ativo novamente no Cluster B, com o histórico de estatísticas e uma lacuna nas estatísticas referente ao período durante o switchover. O Vol3b não estará visível no Cluster A até que outro switchover ocorra:



- Os volumes do MetroCluster que estão inativos, por exemplo, o Vol3b no Cluster A após o switchback, são identificados com a mensagem “Este volume foi excluído”. O volume não foi realmente excluído, mas no momento 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 sobre o volume que estiver ativo naquele momento. Por exemplo, uma pesquisa por "Vol3" retornaria estatísticas e eventos para Vol3b no Cluster A se tiver ocorrido um switchover e Vol3 tiver se tornado ativo no Cluster A.

Entenda a conectividade do cluster em uma configuração do MetroCluster sobre FC no Active IQ Unified Manager

A conectividade entre os clusters em uma configuração MetroCluster over FC pode ter um dos seguintes status: ideal, impactada ou inativa. Entender os status de conectividade permite que você gerencie suas configurações de MetroCluster com

eficácia.

Estado da conectividade	Descrição	Ícone exibido
Ideal	A conectividade entre os clusters na configuração do MetroCluster está normal.	
Afetado	Um ou mais erros comprometem o status da 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 está inacessível.	
Inativo	A conectividade entre os clusters na configuração do MetroCluster está inativa porque um ou ambos os clusters estão inativos ou os clusters estão em modo de failover. Por exemplo, quando o cluster parceiro está inativo devido a um desastre ou quando há um switchover planejado para fins de teste.	Switchover com erros:  Switchover concluído com sucesso: 

Saiba mais sobre o MetroCluster por espelhamento de dados FC no Active IQ Unified Manager

As configurações do MetroCluster over FC oferecem espelhamento de dados e a capacidade adicional de iniciar um failover caso um site inteiro fique indisponível. O status do espelhamento de dados entre os clusters em uma configuração do MetroCluster over FC pode ser Normal ou Espelhamento indisponível. Entender o status permite que você gerencie suas configurações do MetroCluster com eficiência.

Status do espelhamento de dados	Descrição	Ícone exibido
Normal	O espelhamento de dados entre os clusters na configuração do MetroCluster é normal.	

Status do espelhamento de dados	Descrição	Ícone exibido
Espelhamento indisponível	O espelhamento de dados entre os clusters na configuração do MetroCluster está indisponível devido ao switchover. Por exemplo, quando o cluster parceiro está inativo devido a um desastre ou quando há um switchover planejado para fins de teste.	Switchover com erros:  Switchover concluído com sucesso: 

Monitore as configurações do MetroCluster no Active IQ Unified Manager

Você pode monitorar problemas de conectividade em sua configuração do MetroCluster. Os detalhes incluem o status dos componentes e da conectividade em um cluster, bem como o status da conectividade entre os clusters na configuração do MetroCluster. Aqui, você aprenderá a monitorar problemas de conectividade em clusters protegidos por configurações do MetroCluster over FC e do MetroCluster over 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** visualização
- **Proteção** > **Relacionamentos** > **Relacionamento: MetroCluster** visualização

O Unified Manager utiliza alertas de integridade do sistema para indicar o status dos componentes e a conectividade na configuração do MetroCluster.

Antes de começar

- Tanto o cluster local quanto o remoto em uma configuração MetroCluster devem ser adicionados ao Active IQ Unified Manager.
- Em uma configuração do MetroCluster over IP, se houver suporte a um Mediator, o Mediator deverá ser configurado e adicionado ao cluster pela API correspondente.
- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Monitorar problemas de conectividade na configuração do MetroCluster sobre FC

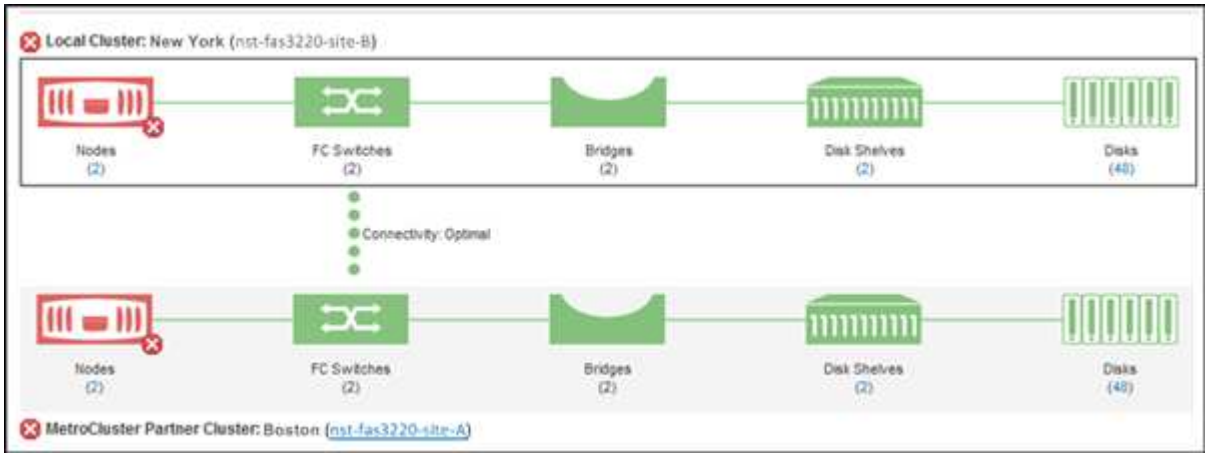
Para clusters em uma configuração do MetroCluster over FC, os gráficos de conectividade são exibidos na página de detalhes **Cluster / Health**. Siga estas etapas.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Clusters**.

   Você verá uma lista de todos os clusters monitorados.

2. Na visualização **Proteção: MetroCluster**, clique no nome do cluster para o qual você deseja visualizar os detalhes da configuração do MetroCluster over FC. Como alternativa, você pode filtrar por clusters em uma configuração do MetroCluster.
3. Na página de detalhes **Cluster / Saúde**, clique na guia **Conectividade do MetroCluster**. A guia **Conectividade do MetroCluster** está disponível apenas para configurações do MetroCluster via FC.



A topologia da configuração do MetroCluster é exibida na área de objetos do cluster correspondente. Você pode usar as informações exibidas na página de detalhes Cluster/Health para corrigir quaisquer problemas de conectividade. Por exemplo, se a conectividade entre o nó e o switch em um cluster estiver inativa, o seguinte ícone será exibido:



Ao posicionar o cursor sobre o ícone, você pode visualizar informações detalhadas sobre o evento gerado.

Se você detectar problemas de conectividade em sua configuração do MetroCluster, deverá fazer login no System Manager ou acessar a ONTAP CLI para resolvê-los.

Para obter mais informações sobre como determinar a integridade do cluster, consulte "Determine a integridade do cluster na configuração do MetroCluster sobre FC".

Monitorar problemas de conectividade na configuração do MetroCluster sobre IP

Para clusters em uma configuração de MetroCluster over IP, os gráficos de conectividade são exibidos na página **Clusters**. Siga estas etapas.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Clusters**.

   Você verá uma lista de todos os clusters monitorados.

2. Na visualização **Proteção: MetroClusters**, clique no nome do cluster para o qual você deseja visualizar os detalhes da configuração do MetroCluster over IP. Como alternativa, você pode filtrar por clusters em uma configuração MetroCluster.
3. Expanda a linha clicando no ícone de cursor v. O ícone de cursor aparece apenas para um cluster protegido pelo MetroCluster em uma configuração over IP.

   Você pode visualizar a topologia dos sites de origem e de espelhamento, bem como o Mediator, se houver, usado para a conexão. Você pode visualizar as seguintes informações:

- Conectividade entre os locais
- Problemas de integridade e disponibilidade, se houver, em ambos os sites
- Problemas relacionados ao Mediator
- Problemas relacionados à replicação.

Os seguintes status são relatados: crítico (), erro () ou normal (). Você também pode visualizar o status agregado da replicação de dados dos dados primários e espelhados na mesma topologia.

No diagrama a seguir, você pode ver que a conectividade entre sites entre os clusters de origem e destino não está disponível, e o Mediator 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 de MetroCluster over IP, você pode clicar no botão **View Event** na mensagem e visualizar os detalhes do evento. Quando você resolver o problema e o evento, o ícone de status nesta topologia voltará ao normal ().
5. Você pode ver mais detalhes de configuração nas seções **MetroCluster Visão geral** e **Proteção** da guia **Configuração** da página de detalhes **Cluster / Saúde**.

Somente para uma configuração do MetroCluster over IP, você pode visualizar a topologia do cluster na página **Clusters**. Para clusters em uma configuração do MetroCluster over FC, a topologia é exibida na guia **MetroCluster Connectivity** na página de detalhes **Cluster / Health**.

Informações relacionadas

- "Página de detalhes de 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 "Relação: visualização da taxa de transferência do último mês".

- Para obter informações sobre a visualização **Relacionamento: todos os relacionamentos**, consulte "Relacionamento: visualizar todos os relacionamentos".

Monitore a replicação do MetroCluster no Active IQ Unified Manager

Você pode monitorar e diagnosticar o estado geral de saúde das conexões lógicas durante o espelhamento dos dados. Você pode identificar problemas ou qualquer risco que interrompa o espelhamento de componentes do cluster, como agregados, nós e máquinas virtuais de storage.

O Unified Manager usa alertas de integridade do sistema para monitorar o status dos componentes e a conectividade na configuração do MetroCluster.

Antes de começar

Tanto o cluster local quanto o cluster remoto na configuração do MetroCluster devem ser adicionados ao Unified Manager

Visualizar a replicação para configurações do MetroCluster over IP

Para configurações do MetroCluster over IP, o status da replicação de dados é exibido na visualização rápida da topologia de um cluster protegido pelo MetroCluster over IP nas seguintes visualizações do painel de navegação esquerdo do Unified Manager:

- **Armazenamento** > **Clusters** > **Proteção: MetroCluster** visualização
- **Proteção** > **Relacionamentos** > **Relacionamento: MetroCluster** visualização

Para informações, consulte "Monitorar problemas de conectividade no MetroCluster over IP".

Visualizar a replicação para o MetroCluster em configurações FC

Siga estas etapas para identificar quaisquer problemas na replicação de dados da configuração MetroCluster over FC.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Clusters**.

   Você vê uma lista dos clusters monitorados.

2. Na visualização **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 local local, na área de objeto do cluster correspondente, com as informações sobre o local remoto onde os dados estão sendo espelhados. Ao posicionar o cursor sobre o ícone, você pode visualizar informações detalhadas sobre o evento gerado.

Você pode usar as informações exibidas na página de detalhes Cluster / Health para corrigir quaisquer problemas de replicação. Se você descobrir problemas de espelhamento na sua configuração do MetroCluster, deverá fazer login no System Manager ou acessar a ONTAP CLI para resolvê-los.

Informações relacionadas

"Página de detalhes de cluster / saúde"

Gerenciar cotas

Saiba mais sobre os limites de cota no Active IQ Unified Manager

Os limites de cota de usuário são valores que o servidor Unified Manager utiliza para avaliar se o consumo de espaço por um usuário está se aproximando do limite ou se atingiu o limite definido pela cota do usuário. Se o limite flexível for ultrapassado ou se o limite rígido for atingido, o servidor 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 os eventos de cota de usuário estão configurados. Os usuários com a função de Application Administrator podem configurar alertas que notificam os destinatários especificados sobre os eventos de cota de usuário ou de grupo de usuários.

Você pode especificar limites de cota usando o ONTAP System Manager ou a ONTAP CLI.

Visualize as quotas de usuários e grupos de usuários no Active IQ Unified Manager

A página de detalhes Storage VM / Health exibe informações sobre as quotas de usuário e de grupo de usuários configuradas na SVM. Você pode ver o nome do usuário ou do grupo de usuários, os limites definidos para os discos e arquivos, o espaço em disco e em arquivos usado e o endereço de e-mail para notificação.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **VMs de armazenamento**.
2. Na visualização **Saúde: Todas as VMs de storage**, selecione uma VM de storage e clique na guia **Cotas de usuário e grupo**.

Informações relacionadas

"Adicionando usuários"

Crie regras para gerar endereços de e-mail no Active IQ Unified Manager

Você pode criar regras para especificar o endereço de e-mail com base na cota de usuário associada a clusters, máquinas virtuais de storage (SVMs), volumes, qtrees, usuários ou grupos de usuários. Uma notificação é enviada para o endereço de e-mail especificado quando ocorre uma violação de cota.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você deve ter revisado as diretrizes na página Regras para gerar endereços de e-mail para cotas de usuário e grupo.

Você deve definir as regras para os 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 o grupo abc e usar o endereço de e-mail dl-$GROUP@$DOMAIN para todos os outros grupos, as regras devem ser listadas na seguinte ordem:

- if ($USER == 'abc') then abc@xyz.com
- se ($GROUP == *) então dl-$GROUP@$DOMAIN

Se nenhum dos critérios das regras que você especificou 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 e-mail de cota**.
2. Insira a regra com base nos seus critérios.
3. Clique em **Validar** para validar a sintaxe da regra.

   Uma mensagem de erro é exibida se a sintaxe da regra estiver incorreta. Você deve corrigir a sintaxe e clicar em **Validate** 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 de storage **VM / Health**.

Crie um formato de notificação por e-mail para cotas de usuários e grupos de usuários no Active IQ Unified Manager

Você pode criar um formato de notificação para os e-mails enviados a um usuário ou grupo de usuários quando houver um problema relacionado à cota (limite flexível ultrapassado ou limite rígido atingido).

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação à esquerda, 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 ver uma prévia da notificação por e-mail.
4. Clique em **Fechar** para fechar a janela de pré-visualização.
5. Modifique o conteúdo da notificação por e-mail, se necessário.
6. Clique em **Salvar**.

Edite os endereços de e-mail de cotas de usuários e grupos no Active IQ Unified Manager

Você pode modificar os endereços de e-mail com base na cota de usuário associada a clusters, máquinas virtuais de armazenamento (SVMs), volumes, qtrees, usuários ou grupos de usuários. Você pode modificar o endereço de e-mail quando desejar 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Você deve ter revisado o "diretrizes para a criação de regras".

Ao editar um endereço de e-mail, as regras para gerar os endereços de e-mail de cota de usuário e de grupo deixam de ser aplicáveis à cota. Para que as notificações sejam enviadas para o endereço de e-mail gerado pelas regras especificadas, você deve excluir o endereço de e-mail e salvar a alteração.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **SVMs**.
2. Na visualização **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 abas.
4. Na caixa de diálogo **Editar endereço de e-mail**, execute a ação apropriada:

Se…	Então…
Deseja que as notificações sejam enviadas para o endereço de e-mail gerado pelas regras especificadas	a. Apague 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 Edit Email Address. O endereço de e-mail gerado pela regra especificada é exibido no campo **Email Address**.
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 os endereços de e-mail de cota de usuário e grupo não são mais aplicáveis à cota.

Entenda melhor as cotas

Saiba mais sobre o processo de cotas do Active IQ Unified Manager

As quotas podem ser flexíveis ou rígidas. As quotas flexíveis fazem com que ONTAP envie uma notificação quando os limites especificados forem excedidos, enquanto as quotas rígidas impedem que uma operação de gravação seja concluída com sucesso quando os limites especificados forem excedidos.

Quando o ONTAP recebe uma solicitação de um usuário ou grupo de usuários para gravar em um FlexVol volume, ele verifica se as cotas estão ativadas nesse volume para o usuário ou grupo de usuários e determina o seguinte:

- Se o limite rígido será atingido

  Caso afirmativo, a operação de gravação falha quando o limite rígido é atingido e a notificação de cota

rígida é enviada.

- Se o limite flexível será ultrapassado

  Em caso afirmativo, a operação de gravação é bem-sucedida quando o limite flexível é ultrapassado e a notificação de cota flexível é enviada.

- Se uma operação de gravação não excederá o limite flexível

  Se sim, a operação de gravação é concluída com êxito e nenhuma notificação é enviada.

Saiba mais sobre cotas no Active IQ Unified Manager

As quotas permitem restringir ou rastrear o espaço de disco e o número de arquivos usados por um usuário, grupo ou qtree. Você especifica as quotas usando o arquivo `/etc/quotas`. As quotas são aplicadas a um volume ou qtree.

Saiba mais sobre cotas no Active IQ Unified Manager

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 monitorar o uso de recursos.

Você especifica uma cota pelos seguintes motivos:

- Para limitar a quantidade de espaço de disco ou o número de arquivos que podem ser usados por um usuário ou grupo, ou que uma qtree pode conter
- Para monitorar a quantidade de espaço de disco ou o número de arquivos usados por um usuário, grupo ou qtree, sem impor um limite
- Para alertar os usuários quando o uso de disco ou de arquivos estiver alto

Descrição das caixas de diálogo de quotas

Utilize a caixa de diálogo Cotas no Active IQ Unified Manager

Você pode usar a opção apropriada na guia User and Group Quotas, na visualização Health: All Storage VMs, para configurar o formato da notificação por e-mail enviada quando ocorre um problema relacionado à cota e para configurar regras que especifiquem endereços de e-mail com base na cota de usuário.

Saiba mais sobre a página Formato de Notificação por E-mail no Active IQ Unified Manager

A página Formato de Notificação por E-mail exibe as regras do e-mail enviado a um usuário ou a um grupo de usuários quando ocorre um problema relacionado à cota (limite flexível ultrapassado ou limite rígido atingido).

A notificação por e-mail é enviada somente quando os seguintes eventos de cota de usuário ou cota de grupo de usuários são gerados: limite flexível de espaço em disco da cota de usuário ou grupo violado, limite flexível de contagem de arquivos da cota de usuário ou grupo violado, limite rígido de espaço em disco da cota de usuário ou grupo atingido ou limite rígido de contagem de arquivos da cota de usuário ou grupo atingido.

- **De**

  Exibe o endereço de e-mail do qual o e-mail é enviado, que você pode modificar. Por padrão, este é o endereço de e-mail especificado na página de 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 da cota e reduzir o número de palavras-chave. No entanto, você não deve modificar as palavras-chave.

  As 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 o volume ao 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 usada pelo usuário ou grupo de usuários.

  - $QUOTA_LIMIT

    Especifica o limite rígido de disco ou o limite rígido de arquivo atingido pelo usuário ou grupo de usuários, e um dos seguintes eventos é gerado:

    - Limite rígido de espaço em disco da cota de usuário ou grupo atingido
    - Limite flexível de espaço em disco da cota de usuário ou grupo atingido
    - Limite rígido de contagem de arquivos da cota de usuário ou grupo atingido
    - Limite flexível de contagem de arquivos da cota de usuário ou grupo atingido

  - $QUOTA_USED

    Especifica o espaço de disco utilizado ou o número de arquivos criados pelo usuário ou grupo de usuários.

  - $QUOTA_USER

    Especifica o nome do usuário ou do grupo de usuários.

Botões de comando

Os botões de comando permitem visualizar, salvar ou cancelar as alterações feitas no formato da notificação por e-mail:

- **Pré-visualização**

Exibe uma pré-visualização do e-mail de notificação.

- **Restaurar para as configurações de fábrica**

  Permite restaurar o formato de notificação para os valores padrão de fábrica.

- **Salvar**

  Salva as alterações feitas no formato da notificação.

Saiba mais sobre as regras de cota de endereços de e-mail no Active IQ Unified Manager

A página "Regras para gerar endereços de e-mail de cota de usuário e grupo" permite criar regras para especificar endereços de e-mail com base na cota de usuário associada a clusters, SVMs, volumes, qtrees, usuários ou grupos de usuários. O sistema envia uma notificação para o endereço de e-mail especificado quando uma cota é excedida.

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. Caso contrário, o critério da próxima regra será considerado, e assim por diante. Cada linha lista uma regra separada. A regra padrão é a última da lista. Você pode alterar a ordem de prioridade das regras. No entanto, não é possível alterar a ordem da regra padrão.

Por exemplo, se você quiser usar o endereço de e-mail qtree1@xyz.com para receber notificações sobre violações de cota para qtree1 e usar o endereço de e-mail admin@xyz.com para todas as outras qtrees, as regras devem ser listadas na seguinte ordem:

- se ($QTREE == 'qtree1') então qtree1@xyz.com
- if ($QTREE == *) then admin@xyz.com

Se nenhum dos critérios das regras que você especificou 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 vírgulas, e as regras não se aplicam à cota.

Como você adiciona comentários

Você pode adicionar comentários para explicar as regras. Use # no início de cada comentário e cada linha deve conter 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 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. As variáveis válidas podem estar em maiúsculas ou minúsculas, mas não podem ser uma combinação de ambas. Por exemplo, $domain e $DOMAIN são válidas, 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. As variáveis válidas podem estar em maiúsculas ou minúsculas, mas não devem ser uma combinação de ambas. Por exemplo, $domain e $DOMAIN são válidas, mas $Domain não é uma variável válida.

Botões de comando

Os botões de comando permitem salvar, validar ou cancelar as regras criadas:

- **Validar**

  Valida a sintaxe da regra criada. Se houver erros durante a validação, a regra que gerou o erro será exibida juntamente com uma mensagem de erro.

- **Restaurar para as configurações 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 gerou o erro é exibida juntamente com uma mensagem de erro.

Solução de problemas

Adicione espaço de disco ao diretório do banco de dados do Unified Manager

Adicione espaço de disco ao diretório do banco de dados no Active IQ Unified Manager

O diretório do banco de dados do Unified Manager contém todos os dados de integridade e desempenho coletados dos sistemas ONTAP. Em algumas circunstâncias, pode ser necessário aumentar 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% de ocupação.

As etapas necessárias para adicionar capacidade ao diretório de dados variam dependendo de se o Unified

Manager está em execução em um servidor VMware ESXi, em um servidor Red Hat Linux ou em um servidor Microsoft Windows.

Adicione espaço ao disco de dados da máquina virtual do Active IQ Unified Manager

Se você precisar aumentar a quantidade de espaço no disco de dados para o banco de dados do Unified Manager, poderá adicionar capacidade após a instalação aumentando o espaço de disco por meio do console de manutenção do Unified Manager.

Antes de começar

- Você precisa ter acesso ao vSphere Client.
- A máquina virtual não deve ter nenhum snapshot armazenado localmente.
- Você precisa ter as credenciais do usuário de manutenção.

Recomendamos que você faça um 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, em seguida, adicione mais capacidade de disco aos dados `disk 3`. Consulte a documentação da VMware para obter detalhes.

   Em alguns casos raros, a implementação do Unified Manager usa o "Disco Rígido 2" como disco de dados em vez do "Disco Rígido 3". Se isso ocorreu na sua implementação, aumente o espaço do disco que tiver maior capacidade. O disco de dados sempre terá mais espaço do que o outro disco.

2. No cliente vSphere, selecione a máquina virtual do Unified Manager e, em seguida, selecione a guia **Console**.
3. Clique na janela do console e, em seguida, faça login no console de manutenção usando seu nome de usuário e senha.
4. No **Menu Principal**, insira o número da opção **Configuração do Sistema**.
5. No **Menu de Configuração do Sistema**, insira o número da opção **Aumentar o Tamanho do Disco de Dados**.

Adicione espaço ao diretório de dados do host Linux no Active IQ Unified Manager

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

Antes de começar

Você deve ter acesso de usuário raiz à máquina Red Hat Enterprise Linux na qual o Unified Manager está instalado.

Recomendamos que você faça backup do banco de dados do Unified Manager antes de aumentar o tamanho do diretório de dados.

Passos

1. Faça login como usuário raiz na máquina Linux na qual você deseja adicionar espaço de disco.

2. Pare o serviço do 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 de disco suficiente para conter os dados no diretório atual `/opt/netapp/data`.
4. Copie o conteúdo e a configuração de privilégios do diretório existente `/opt/netapp/data` para o diretório de dados de backup:

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

5. Se o SE Linux estiver ativado:

   a. Obtenha o tipo do SE Linux para pastas em uma pasta `/opt/netapp/data` existente:

      ```
      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. Aumente 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` a partir de um disco, não tente montar `/opt/netapp/data` como um compartilhamento NFS ou CIFS. Isso porque, nesse caso, ao tentar expandir o espaço de disco, alguns comandos LVM, como `resize` e `extend`, podem não funcionar como esperado.

8. Confirme se o `/opt/netapp/data` proprietário do diretório (mysql) e o grupo (root) permanecem inalterados:

   ```
   ls -ltr /opt/netapp/ | grep data
   ```

   O sistema retorna uma confirmação semelhante à seguinte:

   ```
   drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
   ```

9. Se o SE Linux estiver ativado, confirme se o contexto do `/opt/netapp/data` 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 extra não cause um erro no banco de dados no futuro.
11. Copie o conteúdo de `backup-data` volta para o diretório expandido `/opt/netapp/data`:

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

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

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

13. Inicie o serviço MySQL:

```
systemctl start mysqld
```

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

```
systemctl start ocie ocieau
```

15. Após todos os serviços serem iniciados, exclua a pasta de backup `/backup-data`:

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

Adicione espaço à unidade lógica do servidor Microsoft Windows no Active IQ Unified Manager

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

Antes de começar

Você precisa ter privilégios de administrador do Windows.

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

Passos

1. Faça login como administrador no servidor Windows no qual deseja adicionar espaço de disco.
2. Siga o passo a passo correspondente ao método que deseja usar para adicionar mais espaço:

Opção	Descrição
Em um servidor físico, adicione capacidade à unidade lógica na qual o servidor do Unified Manager está instalado.	Siga os passos descritos no tópico da Microsoft: "Ampliar um Volume Básico"
Em um servidor físico, adicione um disco rígido.	Siga os passos descritos no tópico da Microsoft: "Adicionando discos rígidos"
Em uma máquina virtual, aumente o tamanho de uma partição de disco.	Siga os passos descritos no tópico da VMware: "Aumentar o tamanho de uma partição de disco"

Altere o intervalo de coleta de estatísticas de desempenho no Active IQ Unified Manager

O intervalo de coleta padrão para estatísticas é de 5 minutos. Você pode alterar esse intervalo para 10 ou 15 minutos se perceber que as coletas de clusters grandes não estão sendo concluídas dentro do tempo padrão. Essa configuração afeta a coleta de estatísticas de todos os clusters que esta instância do Unified Manager está monitorando.

Antes de começar

Você precisa ter um ID de usuário e uma senha autorizados para fazer login no console de manutenção do servidor Unified Manager.

O problema de as coletas de estatísticas de desempenho não serem concluídas no prazo é indicado pelas mensagens no 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 nas coletas de estatísticas. Não altere essa 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 que o Unified Manager relata. Por exemplo, os limites de desempenho definidos pelo sistema acionam eventos quando a política é excedida por 30 minutos. Ao usar coletas a cada 5 minutos, a política deve ser excedida por seis coletas consecutivas. Para coletas a cada 15 minutos, a política deve ser excedida por apenas dois períodos de coleta.

Uma mensagem na parte inferior da página de Configuração do Cluster indica o intervalo atual de coleta de dados estatísticos.

Passos

1. Faça 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 sondagem de desempenho** e pressione Enter.
3. Caso seja solicitado, digite novamente a senha do usuário de manutenção.
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 ativa com um provedor de dados externo (como o Graphite), você deve alterar o intervalo de transmissão do provedor de dados para que ele seja igual ou maior que o intervalo de coleta do Unified Manager.

Altere o período de tempo que o Active IQ Unified Manager retém os dados de eventos e desempenho

Por padrão, o Unified Manager armazena dados de eventos e de desempenho por 6 meses para todos os clusters monitorados. Após esse período, os dados mais antigos são excluídos automaticamente para liberar espaço para 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 forma otimizada.

Antes de começar

Você precisa ter a função de Application Administrator.

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 de desempenho resumidos 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:

- Os dados de desempenho antigos são excluídos do banco de dados do Unified Manager após a meia-noite.
- Os dados de eventos antigos são excluídos imediatamente do banco de dados do Unified Manager.
- Os eventos anteriores ao período de retenção não estarão mais disponíveis para visualização na interface de usuário.
- Os locais na interface de usuário em que as estatísticas de desempenho por hora são exibidas ficarão em branco antes do período de retenção.
- Se o período de retenção de eventos exceder o período de retenção de dados de desempenho, uma mensagem será exibida abaixo do controle deslizante de desempenho alertando 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, mova-a para o número de meses pelos quais os dados devem ser retidos e clique em **Salvar**.

Resolver um erro de autenticação desconhecido no Active IQ Unified Manager

Ao executar uma operação relacionada à autenticação, como adicionar, editar, excluir ou testar usuários ou grupos remotos, a seguinte mensagem de erro pode aparecer: `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
- Nome diferenciado de vinculação do serviço de autenticação OpenLDAP

Ação corretiva

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Com base no serviço de autenticação que você selecionou, insira as informações apropriadas para Nome do administrador ou Nome diferenciado de vinculação.
3. Clique em **Test Authentication** para testar a autenticação com os detalhes que você especificou.
4. Clique em **Salvar**.

Resolver o erro "Usuário não encontrado" no Active IQ Unified Manager

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 diferenciado base com um valor incorreto.

Ação corretiva

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Insira as informações apropriadas para o nome diferenciado base.
3. Clique em **Salvar**.

Resolva o problema causado pela adição do LDAP usando outro serviço de autenticação no Active IQ Unified Manager

Ao selecionar Outros como serviço de autenticação, as classes de objeto de usuário e de grupo mantêm 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 sua classe de objeto de usuário LDAP e a sua classe de objeto de grupo forem user e group, respectivamente, execute os seguintes passos:

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 sua classe de objeto de usuário LDAP e a sua classe de objeto de grupo forem posixAccount e posixGroup, respectivamente, execute os seguintes passos:

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação Remota**.
2. No menu suspenso **Authentication Service**, selecione **OpenLDAP** e em seguida selecione **Others**.
3. Preencha os campos de texto.

Se as duas primeiras soluções alternativas não se aplicarem, chame a `option-set` API e defina as `auth.ldap.userObjectClass` e `auth.ldap.groupObjectClass` opções com os valores corretos.

Resolva um problema de rotação de logs do NetApp Manageability SDK no Active IQ Unified Manager

Após adicionar um cluster baseado na API ONTAPI ao Unified Manager em um sistema operacional Windows, o `nmsdk.log`tamanho do arquivo aumenta e ultrapassa o limite de 10 MB.

Causa

Esse problema pode ocorrer se a rotação de logs 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 obter 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

Saiba mais sobre os eventos da plataforma Active IQ no Active IQ Unified Manager

O Unified Manager pode exibir eventos que foram descobertos pela plataforma Active IQ. Esses eventos são criados pela execução de um conjunto de regras em mensagens AutoSupport geradas por todos os sistemas de armazenamento monitorados pelo Unified Manager.

Para obter 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 externo à rede, você precisa carregar as regras manualmente em **Storage Management** > **Event Setup** > **Upload Rules**.

Esses eventos do Active IQ não se sobrepõem aos eventos existentes do Unified Manager e identificam incidentes ou riscos relacionados à configuração do sistema, ao cabeamento, às melhores práticas e aos problemas de disponibilidade.

Para obter mais informações sobre como ativar eventos da plataforma, consulte "Habilitando eventos do portal Active IQ". Para obter mais informações sobre como carregar o arquivo de regras, consulte "Carregando um novo arquivo de regras do Active IQ".

NetApp Active IQ é um serviço baseado em nuvem que fornece análises preditivas e suporte proativo para otimizar as operações do sistema de storage em toda a nuvem híbrida NetApp. Veja "O NetApp Active IQ" para mais informações.

O que são os eventos do Event Management System

Saiba mais sobre eventos do Sistema de Gerenciamento de Eventos no Active IQ Unified Manager

O Sistema de Gerenciamento de Eventos (EMS) coleta dados de eventos de diferentes partes do kernel do ONTAP e fornece mecanismos de encaminhamento de eventos. Esses eventos do ONTAP podem ser relatados como eventos do EMS no Unified Manager. O monitoramento e o gerenciamento centralizados facilitam a configuração de eventos críticos do EMS e notificações de alerta com base nesses eventos.

O endereço do Unified Manager é adicionado como destino de notificação ao cluster quando você adiciona o cluster ao Unified Manager. Um evento do EMS é relatado assim que o evento ocorre no cluster.

Existem dois métodos para receber eventos EMS no Unified Manager:

- Um certo número de eventos importantes do EMS é relatado automaticamente.
- Você pode se inscrever para receber eventos individuais do EMS.

Os eventos do EMS gerados pelo Unified Manager são relatados de forma diferente dependendo do método utilizado para sua geração:

Funcionalidade	Mensagens EMS automáticas	Mensagens EMS assinadas
Eventos EMS disponíveis	Subconjunto de eventos do EMS	Todos os eventos do EMS
Nome da mensagem EMS quando acionada	Nome do evento do Unified Manager (convertido do nome do evento do EMS)	Mensagem não específica no formato "Erro EMS recebido". A mensagem detalhada fornece o formato de notação de ponto do evento EMS real.
Mensagens recebidas	Assim que o cluster for descoberto	Após adicionar cada evento EMS necessário ao Unified Manager e após o próximo ciclo de polling de 15 minutos
Ciclo de vida do evento	O mesmo que outros eventos do Unified Manager: estados novo, confirmado, resolvido e obsoleto	O evento EMS fica obsoleto após a atualização do cluster, 15 minutos após sua criação
Captura eventos durante períodos de inatividade do Unified Manager	Sim, quando o sistema inicia, ele se comunica com cada cluster para obter eventos ausentes	Não
Detalhes do evento	As ações corretivas sugeridas são importadas diretamente do ONTAP para fornecer soluções consistentes	Ações corretivas não disponíveis na página de 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. Os eventos informativos não podem ser gerenciados usando o mesmo ciclo de vida de eventos que outros tipos de gravidade de eventos, no entanto, o evento se torna obsoleto automaticamente se o mesmo volume receber outro evento de erro “Space Issues”.

Eventos EMS que são adicionados automaticamente ao Active IQ Unified Manager

Os seguintes eventos EMS do ONTAP são adicionados automaticamente ao Unified Manager. Esses eventos serão gerados quando acionados em qualquer cluster que o Unified Manager esteja monitorando.

Os seguintes eventos do EMS estão disponíveis ao monitorar clusters que executam 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 de agregado	arl.netra.ca.check.failed	Agregado	Erro
Acesso à camada de nuvem negado para realocação de agregado durante failover de armazenamento	gb.netra.ca.check.failed	Agregado	Erro

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do Unified Manager
FabricPool Ressincronização da replicação espelhada concluída	wafl.ca.resync.complete	Cluster	Erro
FabricPool com espaço quase esgotado	fabricpool.nearly.full	Cluster	Erro
Período de carência do NVMe-oF iniciado	nvmf.graceperiod.start	Cluster	Aviso
Período de carência do NVMe-oF ativo	nvmf.graceperiod.active	Cluster	Aviso
Período de carência do NVMe-oF expirado	nvmf.graceperiod.expired	Cluster	Aviso
LUN destruída	lun.destroy	LUN	Informação
Nuvem AWS MetaDataConnFail	cloud.aws.metadataConnFail	Nó	Erro
Cloud AWS IAMCredsExpired	cloud.aws.iamCredsExpired	Nó	Erro
Cloud AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	Nó	Erro
Cloud AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	Nó	Erro
Nuvem AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	Nó	Informação
Nuvem AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	Nó	Erro
Nuvem AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	Nó	Erro
Host da camada de nuvem não pode ser resolvido	objstore.host.unresolvable	Nó	Erro
Interface de rede entre clusters da camada de nuvem inativa	objstore.interclusterlifDown	Nó	Erro
Solicitação de incompatibilidade de assinatura do Cloud Tier	osc.signatureMismatch	Nó	Erro
Um dos pools de NFSv4 esgotado	Nblade.nfsV4PoolExhaust	Nó	Crítico
Monitoramento de QoS com memória no máximo	qos.monitor.memory.maxed	Nó	Erro
Monitor de QoS com memória reduzida	qos.monitor.memory.abated	Nó	Informação

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do Unified Manager
Destruir NVMeNS	NVMeNS.destroy	Espaço de nomes	Informação
NVMeNS online	NVMeNS.offline	Espaço de nomes	Informação
NVMeNS offline	NVMeNS.online	Espaço de nomes	Informação
NVMeNS sem espaço	NVMeNS.out.of.space	Espaço de nomes	Aviso
Replicação síncrona fora de sincronia	sms.status.out.of.sync	Relação do SnapMirror	Aviso
Replicação síncrona restaurada	sms.status.in.sync	Relação do SnapMirror	Informação
Falha na resincronização automática da replicação síncrona	sms.resync.attempt.failed	Relação do SnapMirror	Erro
Muitas conexões CIFS	Nblade.cifsManyAuths	SVM	Erro
Número máximo de conexões CIFS excedido	Nblade.cifsMaxOpenSameFile	SVM	Erro
Número máximo de conexões CIFS por usuário excedido	Nblade.cifsMaxSessPerUsrConn	SVM	Erro
Conflito de nome NetBIOS do CIFS	Nblade.cifsNbNameConflict	SVM	Erro
Tentativas de conexão a um compartilhamento CIFS inexistente	Nblade.cifsNoPrivShare	SVM	Crítico
A operação de cópia de sombra do CIFS falhou	cifs.shadowcopy.failure	SVM	Erro
Vírus detectado pelo servidor AV	Nblade.vscanVirusDetected	SVM	Erro
Sem conexão com o servidor AV para verificação de vírus	Nblade.vscanNoScannerConn	SVM	Crítico
Nenhum servidor AV registrado	Nblade.vscanNoRegdScanner	SVM	Erro
Sem conexão com servidor AV responsivo	Nblade.vscanConnInactive	SVM	Informação
Servidor AV muito ocupado para aceitar nova solicitação de verificação	Nblade.vscanConnBackPressure	SVM	Erro
Tentativa de usuário não autorizado ao servidor AV	Nblade.vscanBadUserPrivAccess	SVM	Erro
Os constituintes do FlexGroup têm problemas de espaço	flexgroup.constituents.have.space.issues	Volume	Erro

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do Unified Manager
O FlexGroup está com o status do espaço de todos os constituintes OK	flexgroup.constituents.space.status.all.ok	Volume	Informação
FlexGroup Constituintes têm problemas com inodes	flexgroup.constituents.have.inodes.issues	Volume	Erro
FlexGroup Status dos inodes dos constituintes tudo OK	flexgroup.constituents.inodes.status.all.ok	Volume	Informação
Espaço lógico do volume quase cheio	monitor.vol.nearFull.inc.sav	Volume	Aviso
Espaço lógico do volume cheio	monitor.vol.full.inc.sav	Volume	Erro
Espaço lógico normal do volume	monitor.vol.one.ok.inc.sav	Volume	Informação
Volume WAFL AutoSize com falha	wafl.vol.autoSize.fail	Volume	Erro
Volume WAFL AutoSize concluído	wafl.vol.autoSize.done	Volume	Informação
Tempo limite da operação de arquivo READDIR do WAFL	wafl.readdir.expired	Volume	Erro

Inscreva-se nos eventos do ONTAP EMS no Active IQ Unified Manager

Você pode se inscrever para receber eventos do Event Management System (EMS) gerados por sistemas instalados com o software ONTAP. Um subconjunto de eventos EMS é reportado ao Unified Manager automaticamente, mas eventos EMS adicionais são reportados somente se você tiver se inscrito para esses eventos.

Antes de começar

Não se inscreva em eventos do EMS que já são adicionados ao Unified Manager automaticamente, pois isso pode causar confusão ao receber dois eventos para o mesmo problema.

Você pode assinar qualquer número de eventos EMS. Todos os eventos que você assina são validados, e somente os eventos validados são aplicados aos clusters que você está monitorando no Unified Manager. O *ONTAP 9 EMS Event Catalog* fornece informações detalhadas sobre todas as mensagens EMS para a versão especificada do software ONTAP 9. Localize a versão apropriada do *EMS Event Catalog* na página Product Documentation do ONTAP 9 para obter uma lista dos eventos aplicáveis.

"Biblioteca de produtos do ONTAP 9"

Você pode configurar alertas para os eventos EMS do ONTAP aos quais você está inscrito e também pode criar scripts personalizados para executar nesses eventos.

Se você não estiver recebendo os eventos EMS do ONTAP aos quais se inscreveu, pode haver

um problema com a configuração de DNS do cluster que está impedindo o cluster de alcançar o servidor do Unified Manager. Para resolver esse problema, o administrador do cluster deve corrigir a configuração de DNS do cluster e, em seguida, reiniciar o Unified Manager. Isso descarregará os eventos EMS pendentes para o servidor do Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de eventos**.
2. Na página Configuração de eventos, clique no botão **Inscrever-se em eventos EMS**.
3. Na caixa de diálogo "Inscrever-se em eventos EMS", insira o nome do evento EMS do ONTAP ao qual você deseja se inscrever.

   Para ver 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 da assinatura de eventos EMS do ONTAP no Active IQ Unified Manager"

4. Clique em **Add**.

   O evento EMS foi 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 novamente em **Inscrever-se em eventos EMS**.

   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 EMS do ONTAP. Se o nome tiver sido inserido incorretamente, você deverá remover o evento incorreto e adicioná-lo novamente.

Quando o evento do ONTAP EMS ocorre, ele 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 o desfecho do evento ou criar alertas para ele.

Entenda como o Active IQ Unified Manager lida com um evento recebido

Quando o Unified Manager recebe um evento, ele é exibido na página Dashboard, na página de inventário Event Management, nas guias Summary e Explorer da página Cluster/Performance e na página de inventário específica do objeto (por exemplo, a página de inventário Volumes/Health).

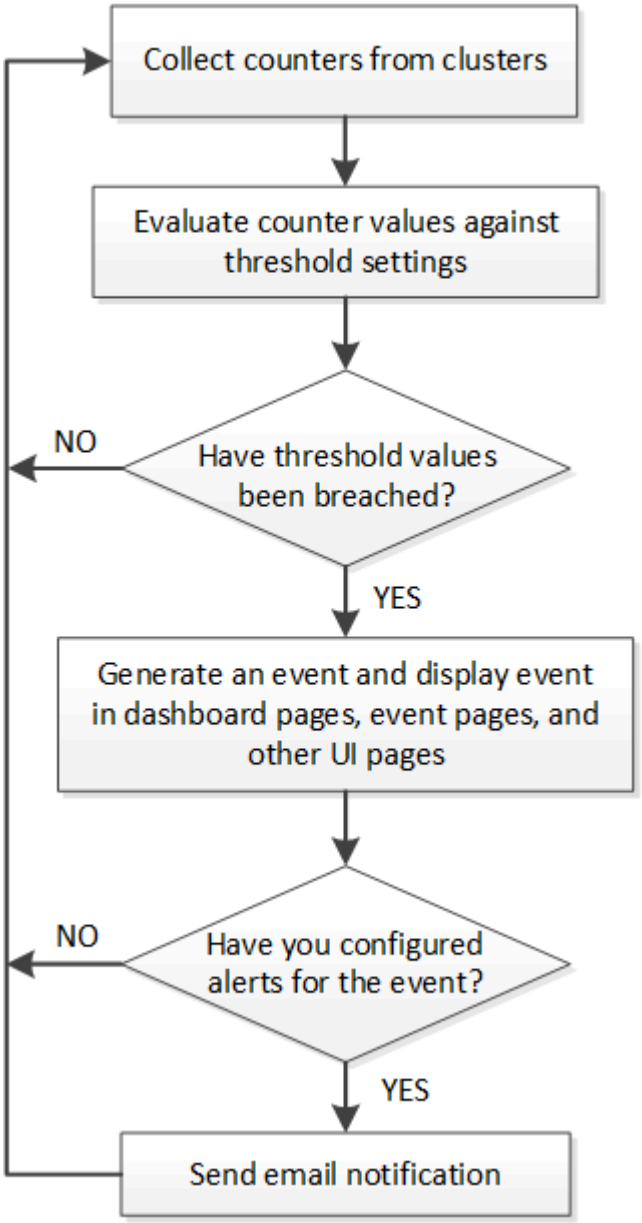
Quando o Unified Manager detecta múltiplas ocorrências contínuas da mesma condição de evento para o mesmo componente do cluster, ele trata todas as ocorrências como um único evento, e não como eventos separados. A duração do evento é incrementada para indicar que ele ainda está ativo.

Dependendo de como você configurar as definições na página de Configuração de Alertas, você pode notificar outros usuários sobre esses eventos. O alerta inicia as seguintes ações:

- Um e-mail sobre o evento pode ser enviado a todos os usuários administradores do Unified Manager.

- O evento pode ser enviado para destinatários adicionais por e-mail.
- Um trap SNMP pode ser enviado para o receptor de traps.
- Você pode executar um script personalizado para realizar uma ação.

Esse fluxo de trabalho é mostrado no diagrama a seguir.



Veja os detalhes do evento no Active IQ Unified Manager

Você pode visualizar detalhes sobre um evento acionado pelo Unified Manager para tomar medidas corretivas. Por exemplo, se houver um evento de integridade "Volume Offline", você pode clicar nesse evento para visualizar os detalhes e executar ações corretivas.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Os detalhes do evento incluem informações como a fonte do evento, a causa do evento e quaisquer notas relacionadas ao evento.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.

   Por padrão, a visualização Todos os eventos ativos exibe os eventos Novos e Reconhecidos (ativos) que foram gerados nos 7 dias anteriores 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 **Visualizar** e selecione no menu de tipos de eventos.
3. Clique no nome do evento para o qual você deseja visualizar os detalhes.

   Os detalhes do evento são exibidos na página de detalhes do evento.

Visualize eventos não atribuídos no Active IQ Unified Manager

Você pode visualizar eventos não atribuídos e em seguida atribuir cada um deles a um usuário que possa resolvê-los.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.

   Por padrão, os eventos Novos e Reconhecidos são exibidos na página de inventário de gerenciamento de eventos.

2. No painel **Filtros**, selecione a opção de filtro **Não atribuído** na área **Atribuído a**.

Reconheça e resolva eventos no Active IQ Unified Manager

Você deve reconhecer um evento antes de começar a trabalhar no problema que gerou o evento, para não continuar recebendo notificações de alerta repetidas. Após tomar as medidas corretivas para um determinado evento, você deve marcá-lo como resolvido.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Você pode reconhecer e resolver vários eventos simultaneamente.

Não é possível confirmar eventos de informação.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.
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 de detalhes do evento, determine a causa do evento. c. Clique em **Acknowledge**. d. Adote as medidas corretivas apropriadas. e. Clique em **Marcar como resolvido**.
Reconheça e marque vários eventos como resolvidos	a. Determine a causa dos eventos na respectiva página de detalhes do evento. b. Selecione os eventos. c. Clique em **Acknowledge**. d. Tome as medidas corretivas apropriadas. e. Clique em **Marcar como resolvido**.

Depois que você marcar o evento como resolvido, ele vai para a lista de eventos resolvidos.

3. **Opcional**: na área **Notes and Updates**, adicione uma nota sobre como você tratou o evento e clique em **Post**.

Atribua eventos a usuários específicos no Active IQ Unified Manager

Você pode atribuir eventos não atribuídos a si mesmo ou a outros usuários, incluindo usuários remotos. Se necessário, você pode reatribuir eventos atribuídos a outro usuário. Por exemplo, quando problemas frequentes ocorrem 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.
2. Na página de inventário **Event Management**, selecione um ou mais eventos que você deseja atribuir.
3. Atribua o evento escolhendo uma das seguintes opções:

Se você deseja atribuir o evento a…	Então faça isso…
Você mesmo	Clique em **Atribuir a** > **Mim**.

Se você deseja atribuir o evento a…	Então faça isso…
Outro usuário	a. Clique em **Atribuir a** > **Outro usuário**. b. Na caixa de diálogo "Assign Owner", insira o nome de 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.

Desative eventos indesejados no Active IQ Unified Manager

Todos os eventos estão ativados por padrão. Você pode desativar eventos globalmente para impedir a geração de notificações para eventos que não são importantes no seu ambiente. Você pode ativar eventos desativados quando desejar voltar a receber notificações para eles.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Ao desativar eventos, os eventos gerados anteriormente no sistema são marcados como obsoletos e os alertas configurados para esses eventos não são acionados. Ao ativar eventos desativados, as notificações para esses eventos são geradas a partir do próximo ciclo de monitoramento.

Quando você desativa um evento para um objeto (por exemplo, o evento `vol offline`) e, posteriormente, o reativa, o Unified Manager não gera novos eventos para objetos que ficaram offline enquanto o evento estava desativado. O Unified Manager gera um novo evento somente quando há uma alteração no estado do objeto após a reativação do evento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de eventos**.
2. Na página **Event Setup**, desative ou ative os eventos escolhendo uma das seguintes opções:

Se você quiser…	Então faça isso…
Desativar eventos	a. Clique em **Desativar**. b. Na caixa de diálogo "Disable Events", selecione a gravidade do evento. c. Na coluna Eventos correspondentes, selecione os eventos que você deseja desativar com base na gravidade do evento e, em seguida, clique na seta para a direita para mover esses eventos para a coluna Desativar eventos. d. Clique em **Salvar e fechar**. e. Verifique se os eventos que você desativou são exibidos na exibição em lista da página Configuração de Eventos.
Ativar eventos	a. Selecione a caixa de seleção do evento, ou eventos, que deseja ativar. b. Clique em **Enable**.

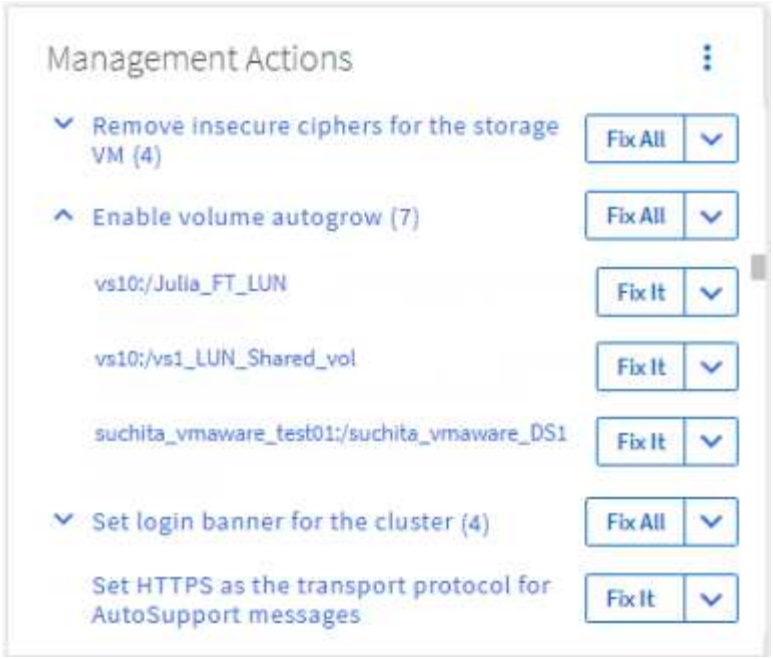
Corrija problemas usando a correção automática no Active IQ Unified Manager

Há certos eventos que o Unified Manager pode diagnosticar minuciosamente e fornecer uma única solução usando o botão **Fix It**. Quando disponíveis, essas soluções são exibidas no Dashboard, na página Event details e na seleção Workload Analysis no menu de navegação à esquerda.

A maioria dos eventos tem várias resoluções possíveis que são exibidas na página de detalhes do evento para que você possa implementar a melhor solução usando o ONTAP System Manager ou a ONTAP CLI. Uma ação **Fix It** está disponível quando o Unified Manager determinou que há uma única resolução para corrigir o problema e que ele pode ser resolvido usando um comando da ONTAP CLI.

Passos

1. Para visualizar os eventos que podem ser corrigidos no **Dashboard**, clique em **Dashboard**.



2. Para resolver qualquer problema que o Unified Manager possa corrigir, clique no botão **Corrigir**. Para corrigir um problema que afeta vários objetos, clique no botão **Corrigir tudo**.

Para obter informações sobre os problemas que podem ser corrigidos por meio de correção automática, consulte "Que problemas o Unified Manager pode resolver".

Ativar e desativar o relatório de eventos do Active IQ no Active IQ Unified Manager

Por padrão, os eventos da plataforma Active IQ são gerados e exibidos na interface de usuário do Unified Manager. Caso você considere que esses eventos geram muito "ruído" ou não queira visualizá-los no Unified Manager, você pode desativar a geração desses eventos. Você pode reativá-los mais tarde, se quiser voltar a receber essas notificações.

Antes de começar

Você precisa ter a função de Application Administrator.

Ao desativar esse recurso, o Unified Manager para de receber eventos da plataforma Active IQ imediatamente.

Ao ativar 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 de AutoSupport de cada cluster.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Configurações de recursos**.
2. Na página **Configurações de recursos**, desative ou ative os eventos da plataforma Active IQ escolhendo uma das seguintes opções:

Se você quiser…	Então faça isso…
Desativar eventos da plataforma Active IQ	No painel **Active IQ Portal Events**, mova o botão deslizante para a esquerda.
Ativar eventos de plataforma do Active IQ	No painel **Active IQ Portal Events**, mova o botão deslizante para a direita.

Carregue um novo arquivo de regras do Active IQ no Active IQ Unified Manager

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 externo à rede, você precisa fazer upload do arquivo de regras manualmente.

As regras do Active IQ também são conhecidas como 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, recomenda-se que você baixe um novo arquivo de regras aproximadamente uma vez por mês do site de suporte da NetApp para garantir que eventos atualizados sejam gerados e que seus sistemas de armazenamento continuem tendo o desempenho ideal.

Antes de começar

- A geração de relatórios de eventos do portal Active IQ deve estar ativada. Esse recurso está ativado por padrão. Para obter mais informações, consulte "Habilitando eventos do portal Active IQ".
- Você precisa 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, acesse o site de suporte da NetApp e baixe o arquivo de regras `.zip` atual.

   O pacote de regras incluído contém o repositório de regras, as 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 base de conhecimento da NetApp não é incluído por padrão com o instalador. Você pode baixar o arquivo *secure_rules.zip* do site de suporte e carregá-lo para visualizar o artigo da base de conhecimento de todas as regras.

2. Transfira o arquivo de regras para uma mídia que você possa levar para a área segura e, em seguida, copie-o para um sistema na área segura.
3. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de eventos**.
4. Na página **Configuração do Evento**, clique no botão **Carregar Regras**.
5. Na caixa de diálogo **Upload Rules**, localize e selecione o arquivo de regras `.zip` que você baixou e clique em **Upload**.

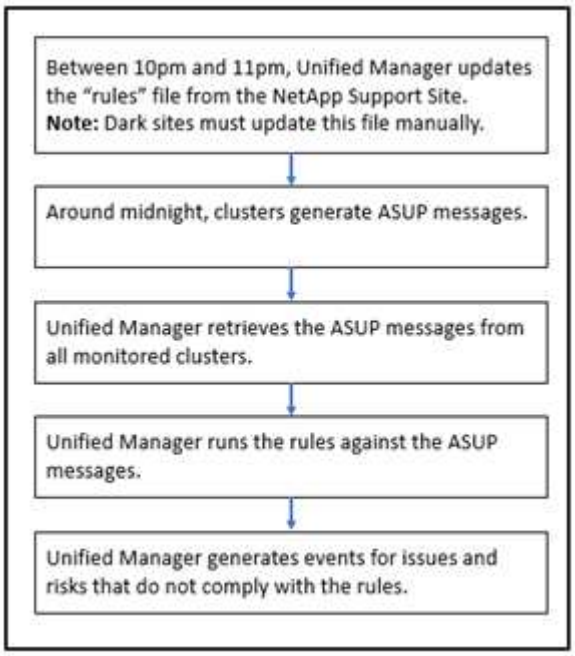
Esse processo pode levar alguns minutos.

O arquivo de regras é descompactado no servidor do Unified Manager. Depois que seus 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 manualmente as regras do AIQCASecure no Active IQ Unified Manager".

Como o Active IQ Unified Manager gera eventos da plataforma Active IQ

Os incidentes e riscos da plataforma Active IQ são convertidos em eventos do Unified Manager, conforme mostrado no diagrama a seguir.

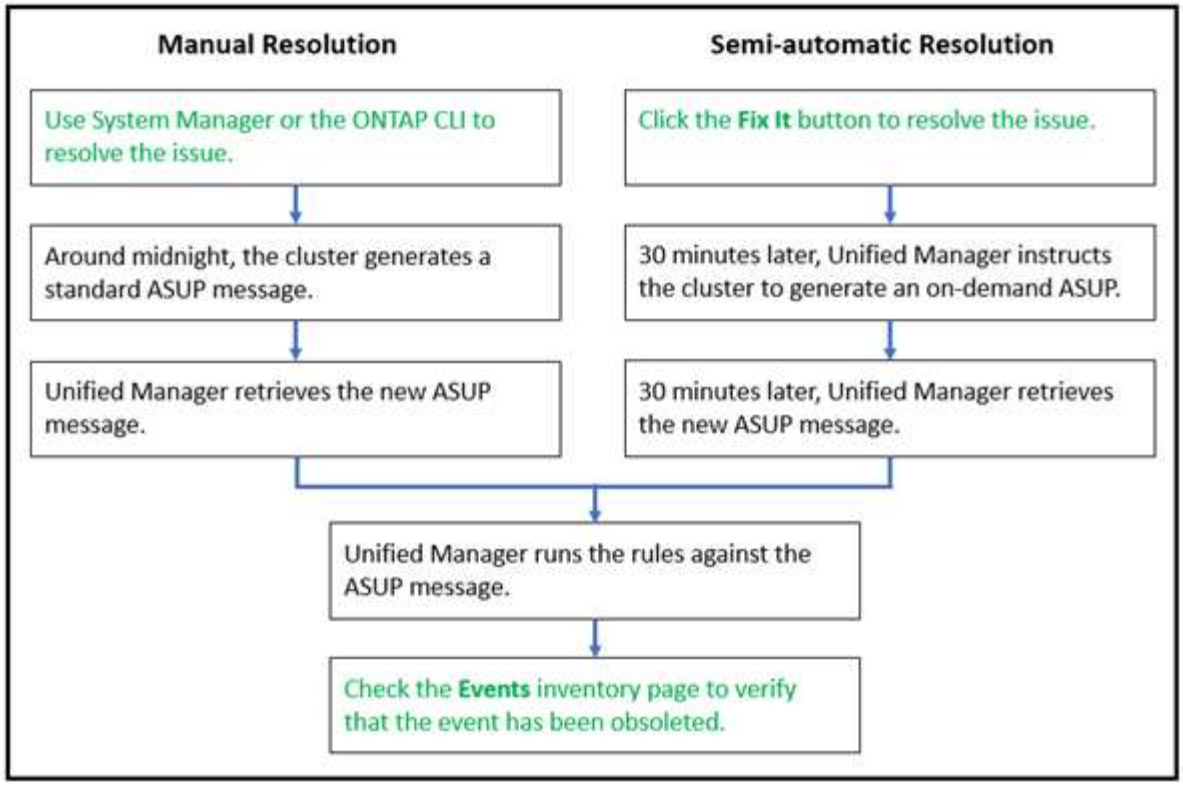


Como você pode ver, o arquivo de regras compilado na plataforma Active IQ é mantido atualizado, as mensagens de cluster AutoSupport são geradas diariamente, e o Unified Manager atualiza a lista de eventos diariamente.

Resolva eventos da plataforma Active IQ no Active IQ Unified Manager

Os incidentes e riscos da plataforma Active IQ são semelhantes a outros eventos do Unified Manager, pois 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 **Fix It**, você pode verificar a resolução em poucas horas.

O diagrama a seguir mostra as ações que você deve executar (em verde) e a ação que o Unified Manager executa (em preto) ao resolver eventos gerados pela plataforma Active IQ.



Ao realizar uma resolução manual, você deve fazer login no System Manager ou na interface de linha de comando do ONTAP para corrigir o problema. Você só poderá verificar o problema depois que o cluster gerar uma nova mensagem do AutoSupport à meia-noite.

Ao executar uma resolução semiautomática usando o botão **Fix It**, você poderá verificar se a correção foi bem-sucedida em poucas horas.

Configure as configurações de retenção de eventos no Active IQ Unified Manager

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 precisa ter a função de Application Administrator.

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 de Retenção de Eventos, mova-o para o número de meses durante os quais os eventos devem ser retidos e clique em **Salvar**.

O que é uma janela de manutenção do Unified Manager

Saiba mais sobre as janelas de manutenção do Active IQ Unified Manager

Você define uma janela de manutenção do Unified Manager para suprimir eventos e alertas durante um período específico quando tiver agendado a manutenção do cluster e

não quiser receber uma enxurrada de notificações indesejadas.

Quando a janela de manutenção começa, um evento "Object Maintenance Window Started" é publicado na página de inventário do Event Management. Esse evento é automaticamente removido quando a janela de manutenção termina.

Durante uma janela de manutenção os eventos relacionados a todos os objetos desse cluster ainda são gerados, mas não aparecem em nenhuma das páginas da interface de usuário, e nenhum alerta ou outro tipo de notificação é enviado para esses eventos. No entanto, você pode visualizar os eventos gerados para todos os objetos de armazenamento durante uma janela de manutenção selecionando uma das opções de visualização na página de inventário de gerenciamento de eventos.

Você pode agendar uma janela de manutenção para iniciar no futuro, pode alterar os horários de início e término de uma janela de manutenção agendada e pode cancelar uma janela de manutenção agendada.

Agende uma janela de manutenção para desativar as notificações de eventos do cluster no Active IQ Unified Manager

Se você tiver um período 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 precisa ter a função de Application Administrator ou Storage Administrator.

Durante uma janela de manutenção, os eventos relacionados a todos os objetos desse 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 que você insere para a janela de manutenção se baseia no horário do servidor 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 da 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 em modo de manutenção e um evento "Object Maintenance Window Started" é gerado.

Alterar ou cancelar uma janela de manutenção no Active IQ Unified Manager

Se você configurou uma janela de manutenção do Unified Manager para ocorrer no futuro, pode alterar os horários de início e término ou cancelar a ocorrência da janela de manutenção.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Cancelar uma janela de manutenção em execução no momento é útil se você concluiu a manutenção do cluster antes do término programado da janela de manutenção e deseja voltar a receber eventos e alertas do cluster.

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 de uma janela de manutenção agendada	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 a hora de término e clique em **Aplicar**.
Cancelar uma janela de manutenção agendada	Selecione o botão deslizante e mova-o para a esquerda.
Cancelar uma janela de manutenção ativa	Selecione o botão deslizante e mova-o para a esquerda.

Visualize os eventos gerados durante uma janela de manutenção no Active IQ Unified Manager

Se necessário, você pode visualizar os eventos gerados para todos os objetos de storage durante uma janela de manutenção do Unified Manager. A maioria dos eventos aparecerá no estado "Obsoleto" assim que a janela de manutenção terminar e todos os recursos do sistema estiverem novamente em funcionamento.

Antes de começar

Pelo menos uma janela de manutenção deve ser concluída antes que qualquer evento esteja disponível.

Os eventos que ocorreram durante uma janela de manutenção não aparecem na página de inventário do Gerenciamento de Eventos por padrão.

Passos

1. No painel de navegação à esquerda, clique em **Eventos**.

   Por padrão, todos os eventos ativos (New e Acknowledged) são exibidos na página de inventário Event Management.

2. No painel Exibir, selecione a opção **Todos os eventos gerados durante a manutenção**.

   É apresentada a lista de eventos acionados durante os últimos 7 dias em todas as sessões de janela de manutenção e em todos os clusters.

3. Se tiver havido várias janelas de manutenção para um único cluster, você poderá clicar no ícone de calendário **Horário de acionamento** e selecionar o período das ocorrências da janela de manutenção que deseja visualizar.

Gerencie eventos de recursos do sistema host no Active IQ Unified Manager

O Unified Manager inclui um serviço que monitora problemas de recursos no sistema host em que o Unified Manager está instalado. Problemas como falta de espaço de 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 de usuário.

Os eventos da estação de gerenciamento indicam um problema no sistema host em que o Unified Manager está instalado. Exemplos de problemas na estação de gerenciamento incluem pouco espaço de disco no sistema host; o Unified Manager não executar um ciclo regular de coleta de dados; e a não conclusão, ou a conclusão tardia, da análise de estatísticas porque a próxima sondagem de coleta foi iniciada.

Diferentemente de todas as outras mensagens de eventos do Unified Manager, esses eventos específicos de aviso e críticos da estação de gerenciamento são exibidos em mensagens de banner.

Etapa

1. Para visualizar as informações sobre eventos da estação de gerenciamento, execute as seguintes ações:

Se você quiser…	Faça isso…
Veja os detalhes do evento	Clique no banner do evento para exibir a página de detalhes do evento, que inclui soluções sugeridas para o problema.
Veja todos os eventos da estação de gerenciamento	a. No painel de navegação à esquerda, clique em **Event Management**. b. No painel Filtros na página de inventário de Gerenciamento de Eventos, clique na caixa Estação de Gerenciamento na lista Tipo de origem.

Entenda melhor os eventos

Estados de eventos no Active IQ Unified Manager

O estado de um evento ajuda você a identificar se uma ação corretiva apropriada é necessária. Um evento pode ser Novo, Reconhecido, Resolvido ou Obsoleto. Observe que tanto os eventos Novos quanto os Reconhecidos são considerados eventos ativos.

Os estados do evento são os seguintes:

- **Novo**

  O estado de um novo evento.

- **Reconhecido**

O estado de um evento quando você o reconheceu.

- **Resolvido**

  O estado de um evento quando ele é marcado como resolvido.

- **Obsoleto**

  O estado de um evento quando ele é corrigido automaticamente ou quando a causa do evento deixa de ser válida.

  Não é possível reconhecer ou resolver um evento obsoleto.

Exemplo de diferentes estados de um evento

Os exemplos a seguir ilustram as alterações manuais e automáticas no estado dos eventos.

Quando o evento Cluster Not Reachable é acionado, o estado do evento é New. Ao reconhecer o evento, o estado do evento muda para Acknowledged. Depois de tomar uma ação corretiva apropriada, você deve marcar o evento como resolvido. O estado do evento então muda para Resolved.

Se o evento "Cluster inacessível" for gerado devido a uma interrupção de energia, quando a energia for restaurada, o cluster começará a funcionar sem qualquer intervenção do administrador. Portanto, o evento "Cluster inacessível" deixa de ser 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 Obsolete ou Resolved. A linha de assunto e o conteúdo do e-mail de um alerta fornecem informações sobre o estado do evento. Um trap SNMP também inclui informações sobre o estado do evento.

Saiba mais sobre os tipos de gravidade de eventos no Active IQ Unified Manager

Cada evento está 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 você não tomar medidas corretivas imediatamente.

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

- **Erro**

  A origem do evento ainda está operando; no entanto, é necessário tomar medidas corretivas para evitar a interrupção do serviço.

- **Aviso**

  A origem do evento apresentou 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 podem não exigir ação corretiva imediata.

Os eventos de aviso de desempenho são enviados com base em limites definidos pelo usuário, definidos pelo sistema ou dinâmicos.

- **Informação**

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

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

Saiba mais sobre os níveis de impacto de eventos no Active IQ Unified Manager

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 pode fazer com que um cluster pare de fornecer dados ao cliente e fique sem espaço para armazenar dados. Eventos com nível de impacto de incidente são os mais graves. Você deve tomar medidas corretivas imediatas para evitar a interrupção do serviço.

- **Risco**

  Um risco é um conjunto de eventos que podem potencialmente fazer com que um cluster pare de fornecer dados ao cliente e fique sem espaço para armazenar dados. Eventos com um nível de impacto de Risco podem causar interrupção do serviço. Ações corretivas podem ser necessárias.

- **Evento**

  Um evento é uma mudança de estado ou status de objetos de armazenamento e seus atributos. Eventos com nível de impacto de Evento são informativos e não exigem ação corretiva.

- **Atualizar**

  Os 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). Você pode querer executar ações corretivas imediatas para alguns desses problemas, enquanto outros podem aguardar até a próxima manutenção programada.

Saiba mais sobre as áreas de impacto de eventos no Active IQ Unified Manager

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 é responsável.

- **Disponibilidade**

  Os eventos de disponibilidade notificam você se um objeto de storage ficar offline, se um serviço de protocolo falhar, se ocorrer um problema com o failover de storage ou se ocorrer um problema com o hardware.

- **Capacidade**

  Os eventos de capacidade notificam você se seus agregados, volumes, LUNs ou namespaces estão se aproximando ou já atingiram um limite de tamanho, ou se a taxa de crescimento é incomum para o seu ambiente.

- **Configuração**

  Os eventos de configuração informam você sobre a descoberta, exclusão, adição, remoção ou renomeação dos seus objetos de storage. Os eventos de configuração têm um nível de impacto "Evento" e um tipo de gravidade "Informação".

- **Desempenho**

  Os eventos de desempenho notificam você sobre condições de recursos, configuração ou atividade em seu cluster que podem afetar negativamente a velocidade de entrada ou recuperação de dados no storage em seus objetos de armazenamento monitorados.

- **Proteção**

  Os eventos de proteção notificam você sobre incidentes ou riscos envolvendo relacionamentos do SnapMirror, problemas com a capacidade de destino, problemas com relacionamentos do SnapVault ou problemas com tarefas de proteção. Qualquer objeto do ONTAP, especialmente agregados, volumes e SVMs, que hospede volumes secundários e relacionamentos de proteção é categorizado na área de impacto da proteção.

- **Segurança**

  Os eventos de segurança notificam você sobre o nível de segurança dos seus clusters do ONTAP, máquinas virtuais de storage (SVMs) e volumes, com base nos parâmetros definidos no "NetApp Guia de Reforço de Segurança para o ONTAP 9".

  Além disso, esta área inclui eventos de atualização relatados pela plataforma Active IQ.

Como o Active IQ Unified Manager calcula o status do objeto

O status de um objeto é determinado pelo evento mais grave que atualmente está no estado Novo ou Reconhecido. Por exemplo, se o status de um objeto for Erro, um dos eventos desse objeto terá o tipo de gravidade Erro. Quando uma ação corretiva é tomada, o estado do evento muda para Resolvido.

Saiba mais sobre eventos de desempenho dinâmico no Active IQ Unified Manager

Para eventos de desempenho dinâmico, a seção Diagnóstico do sistema da página Detalhes do evento lista as principais cargas de trabalho com a maior latência ou uso do componente do cluster que está em contenção.

As estatísticas de desempenho são baseadas no período entre a detecção do evento de desempenho e a última vez em que o evento foi analisado. Os gráficos também exibem estatísticas históricas de desempenho do componente do cluster que está em contenção.

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 contenção. 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 confirmados), a hora da última análise é atualizada.

Os gráficos de latência e atividade exibem os nomes das principais cargas de trabalho quando você posiciona 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*, *agressores* 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".

Ao classificar por desvio máximo de latência, as cargas de trabalho definidas pelo sistema não são exibidas na tabela, pois a latência se aplica apenas às cargas de trabalho definidas pelo usuário. As cargas de trabalho com valores de latência muito baixos não são exibidas na tabela.

Para obter mais informações sobre os limites de desempenho dinâmico, consulte "Analisando eventos a partir de limites de desempenho dinâmicos".

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 antes da última vez em que o evento foi analisado. Os valores reais e esperados para cada carga de trabalho são baseados no momento em que a carga de trabalho esteve envolvida no evento. Por exemplo, uma carga de trabalho pode se envolver em um evento após a detecção do evento, portanto suas estatísticas de desempenho podem não corresponder aos valores no momento da detecção do evento. Por padrão, as cargas de trabalho são ordenadas pelo pico de desvio mais alto 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 é 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 disputa. Nos gráficos, o uso real é representado por uma linha azul. Uma barra vermelha destaca a duração do evento, desde o momento da detecção até o último momento analisado. Para obter 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 de atividades fora do cluster, esta coluna não é exibida.

  - **Utilização de componentes**

    Exibe o histórico de utilização, em porcentagem, dos componentes de processamento de rede, processamento de dados e agregado, ou o histórico de atividade, em porcentagem, do componente do grupo de políticas de QoS. O gráfico não é exibido para os componentes de rede ou de interconexão. Você pode apontar para as estatísticas para ver as estatísticas de uso em um momento específico.

- **Histórico total de gravação em MB/s**

  Somente para o componente Recursos do MetroCluster, exibe a taxa de transferência total de gravação, em megabytes por segundo (MBps), para todas as cargas de trabalho de volume que estão sendo espelhadas no cluster parceiro em uma configuração do MetroCluster.

- **Histórico de Eventos**

  Exibe linhas sombreadas em vermelho para indicar os eventos históricos do componente em contenção. Para eventos obsoletos, o gráfico exibe eventos que ocorreram antes de o evento selecionado ser detectado e depois de sua resolução.

Alterações de configuração detectadas pelo Active IQ 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 consultar os gráficos de desempenho nas páginas do Explorador de Desempenho e na página de Análise de Carga de Trabalho para verificar se o evento de alteração afetou o desempenho do objeto de cluster selecionado. Se a alteração foi detectada simultaneamente ou em um momento próximo a um evento de desempenho, ela pode ter contribuído para o problema que acionou o alerta.

O Unified Manager pode detectar os seguintes eventos de alteração, que são categorizados como eventos informativos:

- Um volume se desloca entre agregados.

  O Unified Manager consegue detectar quando a movimentação está em andamento, concluída ou falhou. Se o Unified Manager estiver inativo durante uma movimentação de volume, ao retornar, ele detectará a movimentação e exibirá um evento de alteração correspondente.

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

- Um nó em um par de HA assume o controle ou faz o giveback do armazenamento do nó parceiro.

  O Unified Manager consegue detectar quando a operação de tomada de controle, tomada de controle parcial ou giveback foi concluída. Se a tomada de controle for causada por um nó em pânico, o Unified Manager não detectará o evento.

- Uma operação de atualização ou reversão do ONTAP é concluída com sucesso.

  A versão anterior e a nova versão são exibidas.

Lista de eventos e tipos de gravidade

Saiba mais sobre eventos agregados no Active IQ Unified Manager

Os eventos de 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 do trap, o nível de impacto, o tipo de origem 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 origem	Gravidade
Agregado Offline(ocumEvtAggregateStateOffline)	Incidente	Agregado	Crítico
Agregado com falha(ocumEvtAggregateStateFailed)	Incidente	Agregado	Crítico
Agregado restrito(ocumEvtAggregateStateRestricted)	Risco	Agregado	Aviso
Agregado em reconstrução(ocumEvtAggregateRaidStateReconstructing)	Risco	Agregado	Aviso
Agregado degradado(ocumEvtAggregateRaidStateDegraded)	Risco	Agregado	Aviso
Camada de nuvem parcialmente acessível(ocumEventCloudTierPartiallyReachable)	Risco	Agregado	Aviso
Nível de nuvem inacessível(ocumEventCloudTierUnreachable)	Risco	Agregado	Erro
Acesso à camada de nuvem negado para realocação de agregado *(arlNetraCaCheckFailed)	Risco	Agregado	Erro
Acesso à camada de nuvem negado para realocação de agregado durante failover de armazenamento *(gbNetraCaCheckFailed)	Risco	Agregado	Erro

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
MetroCluster Agregado deixado para trás(ocumEvtMetroClusterAggregateLeftBehind)	Risco	Agregado	Erro
MetroCluster Espelhamento de agregado degradado(ocumEvtMetroClusterAggregateMirrorDegraded)	Risco	Agregado	Erro

Área de impacto: capacidade

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
Espaço agregado quase cheio(ocumEvtAggregateNearlyFull)	Risco	Agregado	Aviso
Espaço do agregado cheio(ocumEvtAggregateFull)	Risco	Agregado	Erro
Dias do agregado até ficar cheio(ocumEvtAggregateDaysUntilFullSoon)	Risco	Agregado	Erro
Sobrecomprometimento agregado(ocumEvtAggregateOvercommitted)	Risco	Agregado	Erro
Agregado quase sobrecarregado(ocumEvtAggregateAlmostOvercommitted)	Risco	Agregado	Aviso
Reserva de Snapshot do agregado cheia(ocumEvtAggregateSnapReserveFull)	Risco	Agregado	Aviso
Taxa de crescimento do agregado anormal(ocumEvtAggregateGrowthRateAbnormal)	Risco	Agregado	Aviso

Área de impacto: configuração

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
Agregado descoberto(não aplicável)	Evento	Agregado	Informação
Agregado Renomeado(Não aplicável)	Evento	Agregado	Informação
Agregado excluído(não aplicável)	Evento	Nó	Informação

Área de impacto: desempenho

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
Limiar crítico de IOPS do agregado ultrapassado(ocumAggregateIopsIncident)	Incidente	Agregado	Crítico
Limiar de aviso de IOPS agregado ultrapassado(ocumAggregateIopsWarning)	Risco	Agregado	Aviso
Limiar crítico agregado em MB/s ultrapassado(ocumAggregateMbpsIncident)	Incidente	Agregado	Crítico
Limiar de aviso de MB/s do agregado ultrapassado(ocumAggregateMbpsWarning)	Risco	Agregado	Aviso
Limiar crítico de latência do agregado ultrapassado(ocumAggregateLatencyIncident)	Incidente	Agregado	Crítico
Limiar de aviso de latência do agregado ultrapassado(ocumAggregateLatencyWarning)	Risco	Agregado	Aviso
Capacidade de desempenho do agregado usada com limiar crítico violado(ocumAggregatePerfCapacityUsedIncident)	Incidente	Agregado	Crítico

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
Limite de aviso de capacidade de desempenho do agregado usado violado(ocumAggregatePerfCapacityUsedWarning)	Risco	Agregado	Aviso
Limiar crítico de utilização agregada ultrapassado (ocumAggregateUtilizationIncident)	Incidente	Agregado	Crítico
Limite de aviso de utilização agregada ultrapassado (ocumAggregateUtilizationWarning)	Risco	Agregado	Aviso
Limite de sobreutilização de discos agregados ultrapassado (ocumAggregateDisksOverUtilizedWarning)	Risco	Agregado	Aviso
Limiar dinâmico de agregado ultrapassado (ocumAggregateDynamicEventWarning)	Risco	Agregado	Aviso

Saiba mais sobre eventos em cluster no Active IQ Unified Manager

Os eventos de cluster fornecem informações sobre o status dos clusters, permitindo que você os monitore em busca de possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento, o nome do trap, o nível de impacto, o tipo de origem 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 do trap)	Nível de impacto	Tipo de origem	Gravidade
O cluster não possui discos sobressalentes(ocumEvtDisksNoSpares)	Risco	Cluster	Aviso
Cluster não acessível(ocumEvtClusterUnreachable)	Risco	Cluster	Erro

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Falha no monitoramento do cluster(ocumEvtClusterMonitoringFailed)	Risco	Cluster	Aviso
Limites de capacidade de licença do cluster do FabricPool ultrapassados (ocumEvtExternalCapacityTierSpaceFull)	Risco	Cluster	Aviso
Período de carência NVMe-oF iniciado *(nvmfGracePeriodStart)	Risco	Cluster	Aviso
Período de carência NVMe-oF ativo *(nvmfGracePeriodActive)	Risco	Cluster	Aviso
Período de carência do NVMe-oF expirado *(nvmfGracePeriodExpired)	Risco	Cluster	Aviso
Janela de manutenção de objetos iniciada(objectMaintenanceWindowStarted)	Evento	Cluster	Crítico
Janela de manutenção de objeto encerrada(objectMaintenanceWindowEnded)	Evento	Cluster	Informação
MetroCluster Discos sobressalentes deixados para trás(ocumEvtSpareDiskLeftBehind)	Risco	Cluster	Erro
O MetroCluster comutação automática não planejada desativada(ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Risco	Cluster	Aviso
Senha do usuário do cluster alterada *(cluster.passwd.changed)	Evento	Cluster	Informação

Área de impacto: capacidade

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
Limiar de desequilíbrio de capacidade do cluster ultrapassado(ocumConformanceNodeImbalanceWarning)	Risco	Cluster	Aviso
Planejamento de camadas de nuvem de cluster (clusterCloudTierPlanningWarning)	Risco	Cluster	Aviso
FabricPool Ressincronização da replicação espelhada concluída *(waflCaResyncComplete)	Evento	Cluster	Aviso
FabricPool espaço quase cheio *(fabricpoolNearlyFull)	Risco	Cluster	Erro

Área de impacto: configuração

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
Nó adicionado(não aplicável)	Evento	Cluster	Informação
Nó removido(não aplicável)	Evento	Cluster	Informação
Cluster removido(Não aplicável)	Evento	Cluster	Informação
Falha ao adicionar o cluster(Não aplicável)	Evento	Cluster	Erro
Nome do cluster alterado(Não aplicável)	Evento	Cluster	Informação
EMS de emergência recebido (Não aplicável)	Evento	Cluster	Crítico
EMS crítico recebido (Não aplicável)	Evento	Cluster	Crítico
Alerta EMS recebido (Não aplicável)	Evento	Cluster	Erro
Erro EMS recebido (Não aplicável)	Evento	Cluster	Aviso
Aviso do EMS recebido (Não aplicável)	Evento	Cluster	Aviso

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
Debug EMS recebido (Não aplicável)	Evento	Cluster	Aviso
Aviso de EMS recebido (Não aplicável)	Evento	Cluster	Aviso
EMS informativo recebido (Não aplicável)	Evento	Cluster	Aviso

Os eventos do ONTAP EMS são categorizados em três níveis de gravidade de eventos do Unified Manager.

Nível de gravidade do evento do Unified Manager	Nível de gravidade do evento EMS do ONTAP
Crítico	Emergência Crítico
Erro	Alerta
Aviso	Erro Aviso Depurar Aviso Informativo

Área de impacto: desempenho

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
Limiar de desequilíbrio de carga do cluster ultrapassado()	Risco	Cluster	Aviso
Limiar crítico de IOPS do cluster ultrapassado(ocumClusterIopsIncident)	Incidente	Cluster	Crítico
Limiar de aviso de IOPS do cluster ultrapassado(ocumClusterIopsWarning)	Risco	Cluster	Aviso
Limiar crítico de MB/s do cluster ultrapassado(ocumClusterMbpsIncident)	Incidente	Cluster	Crítico

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
Limiar de aviso de MB/s do cluster ultrapassado(ocumClusterMbpsWarning)	Risco	Cluster	Aviso
Limiar dinâmico do cluster ultrapassado(ocumClusterDynamicEventWarning)	Risco	Cluster	Aviso

Área de impacto: segurança

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
AutoSupport Transporte HTTPS desativado(ocumClusterASUPHttpsConfiguredDisabled)	Risco	Cluster	Aviso
Encaminhamento de logs não criptografado(ocumClusterAuditLogUnencrypted)	Risco	Cluster	Aviso
Usuário administrador local padrão ativado(ocumClusterDefaultAdminEnabled)	Risco	Cluster	Aviso
Modo FIPS desativado(ocumClusterFipsDisabled)	Risco	Cluster	Aviso
Banner de login desativado(ocumClusterLoginBannerDisabled)	Risco	Cluster	Aviso
Banner de login alterado(ocumClusterLoginBannerChanged)	Risco	Cluster	Aviso
Destinos de encaminhamento de log alterados(ocumLogForwardDestinationsChanged)	Risco	Cluster	Aviso
Nomes de servidores NTP alterados(ocumNtpServerNamesChanged)	Risco	Cluster	Aviso
Número de servidores NTP é baixo(securityConfigNTPServerCountLowRisk)	Risco	Cluster	Aviso

Nome do evento(nome da armadilha)	Nível de impacto	Tipo de origem	Gravidade
Comunicação entre pares do cluster não criptografada(ocumClusterPeerEncryptionDisabled)	Risco	Cluster	Aviso
O SSH está usando cifras inseguras(ocumClusterSSHInsecure)	Risco	Cluster	Aviso
Protocolo Telnet ativado(ocumClusterTelnetEnabled)	Risco	Cluster	Aviso
As senhas de algumas contas de usuário do ONTAP usam a função de hash MD5 menos segura(ocumClusterMD5PasswordHashUsed)	Risco	Cluster	Aviso
O cluster usa um certificado autoassinado(ocumClusterSelfSignedCertificate)	Risco	Cluster	Aviso
O Shell Remoto do Cluster está ativado(ocumClusterRshDisabled)	Risco	Cluster	Aviso
O certificado do cluster está prestes a expirar(ocumEvtClusterCertificateAboutToExpire)	Risco	Cluster	Aviso
Certificado do cluster expirado(ocumEvtClusterCertificateExpired)	Risco	Cluster	Erro

Saiba mais sobre eventos de disco no Active IQ Unified Manager

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 trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Discos Flash - Blocos de reserva quase esgotados(ocumEvtClusterFlashDiskFewerSpareBlockError)	Risco	Cluster	Erro
Discos Flash - Sem Blocos Sobressalentes(ocumEvtClusterFlashDiskNoSpareBlockCritical)	Incidente	Cluster	Crítico
Alguns discos não atribuídos(ocumEvtClusterUnassignedDisksSome)	Risco	Cluster	Aviso
Alguns discos com falha(ocumEvtDisksSomeFailed)	Incidente	Cluster	Crítico

Saiba mais sobre eventos de enclausuramento no Active IQ Unified Manager

Os eventos de gabinetes fornecem informações sobre o status dos gabinetes de discos em 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 do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
As ventoinhas da gaveta de discos falharam(ocumEvtShelfFanFailed)	Incidente	Gaveta de armazenamento	Crítico
As fontes de alimentação do compartimento de discos falharam(ocumEvtShelfPowerSupplyFailed)	Incidente	Gaveta de armazenamento	Crítico

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Multipath do compartimento de discos 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 do compartimento de discos(ocumDiskShelfConnectivityPathFailure)	Risco	Gaveta de armazenamento	Aviso

Área de impacto: configuração

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Compartimento de discos detectado(não aplicável)	Evento	Nó	Informação
Prateleiras de disco removidas(Não aplicável)	Evento	Nó	Informação

Saiba mais sobre eventos de ventoinhas no Active IQ Unified Manager

Os eventos de ventoinhas fornecem informações sobre o status das ventoinhas nos nós do seu data center, permitindo que você monitore possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Uma ou mais ventoinhas com falha(ocumEvtFansOneOrMoreFailed)	Incidente	Nó	Crítico

Saiba mais sobre eventos de flash card no Active IQ Unified Manager

Os eventos de placas flash fornecem informações sobre o status das placas flash instaladas 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 do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Placas flash offline (ocumEvtFlashCardOffline)	Incidente	Nó	Crítico

Saiba mais sobre eventos de inodes no Active IQ Unified Manager

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 do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: capacidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Inodes quase cheios(ocumEvtInodesAlmostFull)	Risco	Volume	Aviso
Inodes cheios (ocumEvtInodesFull)	Risco	Volume	Erro

Eventos de interface de rede no Active IQ Unified Manager

Os eventos da interface de rede fornecem informações sobre o status da sua interface de rede (LIFs), permitindo que você monitore possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Status da interface de rede inativo(ocumEvtLifStatusDown)	Risco	Interface	Erro

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Status da interface de rede FC/FCoE inativo(ocumEvtFCLifStatusDown)	Risco	Interface	Erro
Failover da interface de rede não é possível(ocumEvtLifFailoverNotPossible)	Risco	Interface	Aviso
Interface de rede não está na porta inicial(ocumEvtLifNotAtHomePort)	Risco	Interface	Aviso

Área de impacto: configuração

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Rota da interface de rede não configurada(Não aplicável)	Evento	Interface	Informação

Área de impacto: desempenho

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limiar crítico de MB/s da interface de rede ultrapassado(ocumNetworkLifMbpsIncident)	Incidente	Interface	Crítico
Limiar de aviso de MB/s da interface de rede ultrapassado(ocumNetworkLifMbpsWarning)	Risco	Interface	Aviso
Limiar crítico de MB/s da interface de rede FC ultrapassado(ocumFcpLifMbpsIncident)	Incidente	Interface	Crítico
Limiar de aviso de MB/s da interface de rede FC ultrapassado(ocumFcpLifMbpsWarning)	Risco	Interface	Aviso
Interface de rede NVMf FC MB/s limiar crítico ultrapassado(ocumNvmfFcLifMbpsIncident)	Incidente	Interface	Crítico

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
NVMf FC interface de rede MB/s aviso de limite ultrapassado(ocumNvmfFcLifMbpsWarning)	Risco	Interface	Aviso

Saiba mais sobre os eventos LUN no Active IQ Unified Manager

Os eventos de LUN fornecem informações sobre o status de seus LUNs, permitindo que você monitore possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem 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 do trap)	Nível de impacto	Tipo de origem	Gravidade
LUN offline (ocumEvtLunOffline)	Incidente	LUN	Crítico
LUN destruída *(lunDestroy)	Evento	LUN	Informação
LUN mapeado com sistema operacional não compatível em igroup(igroupUnsupportedOsType)	Incidente	LUN	Aviso
Caminho único ativo para acessar LUN(ocumEvtLunSingleActivePath)	Risco	LUN	Aviso
Não há caminhos ativos para acessar LUN(ocumEvtLunNotReachable)	Incidente	LUN	Crítico
Não há caminhos otimizados para acessar LUN(ocumEvtLunOptimizedPathInactive)	Risco	LUN	Aviso
Não há caminhos para acessar o LUN do parceiro de HA(ocumEvtLunHaPathInactive)	Risco	LUN	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Não há caminho para acessar o LUN a partir de um nó no par HA(ocumEvtLunNodePathStatusDown)	Risco	LUN	Erro

Área de impacto: capacidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Espaço insuficiente para a cópia Snapshot da LUN(ocumEvtLunSnapshotNotPossible)	Risco	Volume	Aviso

Área de impacto: configuração

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
LUN mapeado com sistema operacional não compatível em igroup(igroupUnsupportedOsType)	Risco	LUN	Aviso

Área de impacto: desempenho

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limiar crítico de IOPS da LUN ultrapassado(ocumLunIopsIncident)	Incidente	LUN	Crítico
Limiar de aviso de IOPS da LUN ultrapassado(ocumLunIopsWarning)	Risco	LUN	Aviso
Limiar crítico de LUN MB/s ultrapassado(ocumLunMbpsIncident)	Incidente	LUN	Crítico
Limiar de aviso de MB/s da LUN ultrapassado(ocumLunMbpsWarning)	Risco	LUN	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Latência de LUN ms/op Limiar crítico ultrapassado(ocumLunLatencyIncident)	Incidente	LUN	Crítico
Limite de aviso de latência de LUN em ms/op ultrapassado(ocumLunLatencyWarning)	Risco	LUN	Aviso
A latência de LUN e o limite crítico de IOPS foram ultrapassados(ocumLunLatencyIopsIncident)	Incidente	LUN	Crítico
Limiar de aviso de latência de LUN e IOPS ultrapassado(ocumLunLatencyIopsWarning)	Risco	LUN	Aviso
Latência de LUN e limite crítico de MB/s atingido(ocumLunLatencyMbpsIncident)	Incidente	LUN	Crítico
Limite de aviso de latência da LUN e MB/s ultrapassado(ocumLunLatencyMbpsWarning)	Risco	LUN	Aviso
Latência de LUN e capacidade de desempenho do agregado usada: limite crítico ultrapassado(ocumLunLatencyAggregatePerfCapacityUsedIncident)	Incidente	LUN	Crítico
Latência da LUN e aviso de violação do limite de capacidade de desempenho agregada usada (ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risco	LUN	Aviso
A latência da LUN e a utilização do agregado ultrapassaram o limite crítico(ocumLunLatencyAggregateUtilizationIncident)	Incidente	LUN	Crítico

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limiar de aviso de latência e utilização agregada de LUN ultrapassado(ocumLunLatencyAggregateUtilizationWarning)	Risco	LUN	Aviso
Latência da LUN e uso da capacidade de desempenho do nó, limite crítico excedido(ocumLunLatencyNodePerfCapacityUsedIncident)	Incidente	LUN	Crítico
Limite de aviso de latência da LUN e capacidade de desempenho do nó usada excedido(ocumLunLatencyNodePerfCapacityUsedWarning)	Risco	LUN	Aviso
Latência da LUN e capacidade de desempenho do nó usada: limite crítico de takeover excedido(ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incidente	LUN	Crítico
Latência da LUN e capacidade de desempenho do nó usada - limite de aviso de tomada de controle ultrapassado(ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risco	LUN	Aviso
A latência do LUN e a utilização do nó atingiram o limite crítico(ocumLunLatencyNodeUtilizationIncident)	Incidente	LUN	Crítico
Limite de aviso de latência da LUN e utilização do nó excedido(ocumLunLatencyNodeUtilizationWarning)	Risco	LUN	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limiar de aviso de IOPS máximo do LUN de QoS ultrapassado(ocumQosLunMaxIopsWarning)	Risco	LUN	Aviso
Limiar de aviso de QoS LUN Max MB/s ultrapassado(ocumQosLunMaxMbpsWarning)	Risco	LUN	Aviso
Limite de latência da LUN da carga de trabalho ultrapassado conforme definido pela Política de Nível de Serviço de Desempenho(ocumConformanceLatencyWarning)	Risco	LUN	Aviso

Saiba mais sobre eventos da estação de gerenciamento no Active IQ Unified Manager

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 do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: configuração

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	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
Servidor de gerenciamento com pouca memória(ocumEvtUnifiedManagerMemoryLow)	Risco	Estação de gerenciamento	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Servidor de gerenciamento quase sem memória(ocumEvtUnifiedManagerMemoryAlmostOut)	Incidente	Estação de gerenciamento	Crítico
O tamanho do arquivo de log do MySQL aumentou; é necessário reiniciar (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
O certificado do servidor Syslog está prestes a expirar	Risco	Estação de gerenciamento	Aviso
Certificado do servidor Syslog expirado	Risco	Estação de gerenciamento	Erro
Arquivo de registro de auditoria adulterado	Risco	Estação de gerenciamento	Aviso
Arquivo de registro de auditoria excluído	Risco	Estação de gerenciamento	Aviso
Erro de conexão com o 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 do trap)	Nível de impacto	Tipo de origem	Gravidade
A análise de dados de desempenho é afetada(ocumEvtUnifiedManagerDataMissingAnalyze)	Risco	Estação de gerenciamento	Aviso
A coleta de dados de desempenho foi afetada(ocumEvtUnifiedManagerDataMissingCollection)	Incidente	Estação de gerenciamento	Crítico

Esses dois últimos eventos de desempenho estavam disponíveis apenas para o Unified Manager 7.2. Se algum desses eventos existir no estado "New" e você atualizar para uma

> versão mais recente do software do Unified Manager, os eventos não serão removidos automaticamente. Você precisará movê-los manualmente para o estado "Resolved".

Saiba mais sobre os eventos Bridge do MetroCluster no Active IQ Unified Manager

Os eventos de bridge do MetroCluster fornecem informações sobre o status das bridges, permitindo que você monitore possíveis problemas em uma configuração MetroCluster over FC. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Ponte inacessível(ocumEvtBridgeUnreachable)	Incidente	Bridge do MetroCluster	Crítico
Temperatura da ponte anormal(ocumEvtBridgeTemperatureAbnormal)	Incidente	Bridge do MetroCluster	Crítico

Saiba mais sobre os eventos de conectividade do MetroCluster no Active IQ Unified Manager

Os eventos de conectividade fornecem informações sobre a conectividade entre os componentes de um cluster e entre clusters em configurações MetroCluster over FC e MetroCluster over IP, para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem e a gravidade.

Eventos comuns em ambas as configurações

Esses eventos de conectividade são comuns tanto para as configurações do MetroCluster sobre FC quanto para as do MetroCluster sobre IP.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Todos os links entre parceiros do MetroCluster estão inativos(ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Incidente	Relacionamento do MetroCluster	Crítico

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
O MetroCluster não consegue acessar os parceiros pela rede de peering(ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Incidente	Relacionamento do MetroCluster	Crítico
O MetroCluster teve a capacidade de recuperação de desastres afetada (ocumEvtMetroClusterDRStatusImpacted)	Risco	Relacionamento do MetroCluster	Crítico
A configuração do MetroCluster foi comutada (ocumEvtMetroClusterDRStatusImpacted)	Risco	Relacionamento do MetroCluster	Aviso

Configuração do MetroCluster over FC

Esses eventos dizem respeito às configurações do MetroCluster over FC.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Todos os links entre switches estão inativos(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Incidente	Conexão entre switches do MetroCluster	Crítico
Link da ponte FC-SAS para a pilha de armazenamento inativo(ocumEvtBridgeSasPortDown)	Incidente	MetroCluster conexão da pilha de pontes	Crítico
MetroCluster configuração parcialmente comutada(ocumEvtMetroClusterDRStatusPartiallyImpacted)	Risco	Relacionamento do MetroCluster	Erro
Node To FC Switch todos os links de interconexão FC-VI estão inativos(ocumEvtMccNodeSwitchFcviLinksDown)	Incidente	Conexão do switch de nó do MetroCluster	Crítico

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Um ou mais links de iniciador FC do nó para o switch FC estão inativos(ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Risco	Conexão do switch de nó do MetroCluster	Aviso
Todos os links do iniciador FC do nó para o switch FC inativos(ocumEvtMccNodeSwitchFcLinksDown)	Incidente	Conexão do switch de nó do MetroCluster	Crítico
Link FC do switch para a ponte FC-SAS inativo (ocumEvtMccSwitchBridgeFcLinksDown)	Incidente	MetroCluster conexão de bridge do switch	Crítico
Todos os links FC VI InterConnect entre nós inativos (ocumEvtMccInterNodeLinksDown)	Incidente	Conexão entre nós	Crítico
Entre nós, um ou mais links FC VI InterConnect inativos (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risco	Conexão entre nós	Aviso
Link do nó para a ponte inativo (ocumEvtMccNodeBridgeLinksDown)	Incidente	Conexão da bridge do nó	Crítico
Todos os links SAS do nó para a pilha de armazenamento estão inativos (ocumEvtMccNodeStackLinksDown)	Incidente	Conexão da pilha de nós	Crítico
Nó para pilha de armazenamento uma ou mais conexões SAS inativas (ocumEvtMccNodeStackLinksOneOrMoreDown)	Risco	Conexão da pilha de nós	Aviso

Configuração do MetroCluster over IP

Esses eventos dizem respeito ao MetroCluster over IP.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
O MetroCluster o status da conectividade IP entre sites está inativo (mccIntersiteconnectivityStatusDown)	Risco	Relacionamento do MetroCluster	Crítico
Conexão offline do nó IP ao switch do MetroCluster (mccIpPortStatusOffline)	Risco	Nó	Erro

Saiba mais sobre os eventos de switch do MetroCluster no Active IQ Unified Manager

Os eventos de switch do MetroCluster para configurações MetroCluster over 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 do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Temperatura anormal do switch(ocumEvtSwitchTemperatureAbnormal)	Incidente	Switch do MetroCluster	Crítico
Switch inacessível(ocumEvtSwitchUnreachable)	Incidente	Switch do MetroCluster	Crítico
As ventoinhas do Switch falharam(ocumEvtSwitchFansOneOrMoreFailed)	Incidente	Switch do MetroCluster	Crítico
As fontes de alimentação do switch falharam(ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Incidente	Switch do MetroCluster	Crítico
Falha nos sensores de temperatura do switch(ocumEvtSwitchTemperatureSensorFailed) Este evento se aplica apenas a switches Cisco.	Incidente	Switch do MetroCluster	Crítico

Saiba mais sobre eventos de namespace NVMe no Active IQ Unified Manager

Os eventos de namespace NVMe fornecem informações sobre o status dos seus namespaces, permitindo que você monitore possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem 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 do trap)	Nível de impacto	Tipo de origem	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
Destruir NVMeNS *(nvmeNamespaceDestroy)	Evento	Espaço de nomes	Informação

Área de impacto: desempenho

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limiar crítico de IOPS do namespace NVMe atingido(ocumNvmeNamespaceIopsIncident)	Incidente	Espaço de nomes	Crítico
Aviso de limite de IOPS do namespace NVMe atingido(ocumNvmeNamespaceIopsWarning)	Risco	Espaço de nomes	Aviso
Limiar crítico de MB/s do namespace NVMe atingido(ocumNvmeNamespaceMbpsIncident)	Incidente	Espaço de nomes	Crítico
Limiar de aviso de MB/s do namespace NVMe ultrapassado(ocumNvmeNamespaceMbpsWarning)	Risco	Espaço de nomes	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Latência do namespace NVMe ms/op limite crítico atingido(ocumNvmeNamespaceLatencyIncident)	Incidente	Espaço de nomes	Crítico
Latência do namespace NVMe ms/op: limite de aviso excedido(ocumNvmeNamespaceLatencyWarning)	Risco	Espaço de nomes	Aviso
Limiar crítico de latência e IOPS do namespace NVMe ultrapassado(ocumNvmeNamespaceLatencyIopsIncident)	Incidente	Espaço de nomes	Crítico
Limiar de aviso de latência e IOPS do namespace NVMe ultrapassado(ocumNvmeNamespaceLatencyIopsWarning)	Risco	Espaço de nomes	Aviso
Latência do namespace NVMe e limite crítico de MB/s excedido(ocumNvmeNamespaceLatencyMbpsIncident)	Incidente	Espaço de nomes	Crítico
Latência do namespace NVMe e limite de aviso de MB/s ultrapassado(ocumNvmeNamespaceLatencyMbpsWarning)	Risco	Espaço de nomes	Aviso

Saiba mais sobre eventos de nó no Active IQ Unified Manager

Os eventos de 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 trap, o nível de impacto, o tipo de origem 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 do trap)	Nível de impacto	Tipo de origem	Gravidade
Espaço do volume raiz do nó quase cheio(ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risco	Nó	Aviso
Nuvem AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	Risco	Nó	Erro
Nuvem AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	Risco	Nó	Erro
Cloud AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	Risco	Nó	Erro
Nuvem AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	Risco	Nó	Erro
Cloud AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	Evento	Nó	Informação
Nuvem AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	Risco	Nó	Erro
Nuvem AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	Risco	Nó	Erro
Host de nível de nuvem não resolvido *(ocumObjstoreHostUnresolvable)	Risco	Nó	Erro
Interface de rede intercluster da camada de nuvem inativa *(ocumObjstoreInterClusterLifDown)	Risco	Nó	Erro
Um dos pools do NFSv4 esgotado *(nbladeNfsv4PoolEXhaust)	Incidente	Nó	Crítico

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Solicitação de assinatura de nível de nuvem incompatível *(oscSignatureMismatch)	Risco	Nó	Erro

Área de impacto: capacidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Monitoramento de QoS com memória no máximo *(ocumQosMonitorMemoryMaxed)	Risco	Nó	Erro
Memória do monitor de QoS reduzida *(ocumQosMonitorMemoryAbated)	Evento	Nó	Informação

Área de impacto: configuração

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Nó renomeado(não aplicável)	Evento	Nó	Informação

Área de impacto: desempenho

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limiar crítico de IOPS do nó atingido(ocumNodeIopsIncident)	Incidente	Nó	Crítico
Limiar de aviso de IOPS do nó ultrapassado(ocumNodeIopsWarning)	Risco	Nó	Aviso
Limiar crítico de MB/s do nó ultrapassado(ocumNodeMbpsIncident)	Incidente	Nó	Crítico
Limiar de aviso de MB/s do nó ultrapassado(ocumNodeMbpsWarning)	Risco	Nó	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Latência do nó ms/op limiar crítico ultrapassado(ocumNodeLatencyIncident)	Incidente	Nó	Crítico
Limiar de aviso de latência do nó em ms/op excedido(ocumNodeLatencyWarning)	Risco	Nó	Aviso
Violação do limite crítico da capacidade de desempenho do nó usada(ocumNodePerfCapacityUsedIncident)	Incidente	Nó	Crítico
Limite de aviso de capacidade de desempenho do nó usada violado(ocumNodePerfCapacityUsedWarning)	Risco	Nó	Aviso
Capacidade de desempenho do nó utilizada - Limiar crítico de tomada de controle ultrapassado(ocumNodePerfCapacityUsedTakeoverIncident)	Incidente	Nó	Crítico
Capacidade de desempenho do nó usada - limite de aviso de takeover violado(ocumNodePerfCapacityUsedTakeoverWarning)	Risco	Nó	Aviso
Limite crítico de utilização do nó excedido (ocumNodeUtilizationIncident)	Incidente	Nó	Crítico
Limite de aviso de utilização de nó ultrapassado (ocumNodeUtilizationWarning)	Risco	Nó	Aviso
O limite de sobreutilização do par HA de nós foi ultrapassado (ocumNodeHaPairOverUtilizedInformation)	Evento	Nó	Informação

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limite de fragmentação do disco do nó ultrapassado (ocumNodeDiskFragmentationWarning)	Risco	Nó	Aviso
Limite de capacidade de desempenho utilizado ultrapassado (ocumNodeOverUtilizedWarning)	Risco	Nó	Aviso
Limiar dinâmico do nó ultrapassado (ocumNodeDynamicEventWarning)	Risco	Nó	Aviso

Área de impacto: segurança

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
ID do aviso: NTAP-<*advisory ID*>(ocumx)	Risco	Nó	Crítico

Saiba mais sobre eventos de bateria NVRAM no Active IQ Unified Manager

Os eventos de 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 do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Bateria de NVRAM fraca(ocumEvtNvramBatteryLow)	Risco	Nó	Aviso
Bateria da NVRAM descarregada(ocumEvtNvramBatteryDischarged)	Risco	Nó	Erro
Bateria da NVRAM excessivamente carregada(ocumEvtNvramBatteryOverCharged)	Incidente	Nó	Crítico

Saiba mais sobre eventos de porta no Active IQ Unified Manager

Os eventos de porta fornecem o status das portas do cluster para que você possa monitorar alterações ou problemas na porta, como por exemplo se a porta está inativa.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Status da porta inativa(ocumEvtPortStatusDown)	Incidente	Nó	Crítico

Área de impacto: desempenho

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limite crítico de MB/s da porta de rede atingido(ocumNetworkPortMbpsIncident)	Incidente	Porta	Crítico
Limite de aviso de MB/s da porta de rede ultrapassado(ocumNetworkPortMbpsWarning)	Risco	Porta	Aviso
Limite crítico de MB/s da porta FCP atingido(ocumFcpPortMbpsIncident)	Incidente	Porta	Crítico
Aviso de limite de MB/s da porta FCP ultrapassado(ocumFcpPortMbpsWarning)	Risco	Porta	Aviso
Limite crítico de utilização da porta de rede ultrapassado(ocumNetworkPortUtilizationIncident)	Incidente	Porta	Crítico
Limiar de aviso de utilização da porta de rede ultrapassado(ocumNetworkPortUtilizationWarning)	Risco	Porta	Aviso
Utilização da porta FCP: limite crítico ultrapassado(ocumFcpPortUtilizationIncident)	Incidente	Porta	Crítico

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limite de aviso de utilização de porta FCP ultrapassado(ocumFcpPortUtilizationWarning)	Risco	Porta	Aviso

Saiba mais sobre eventos relacionados a fontes de alimentação no Active IQ Unified Manager

Os eventos relacionados às fontes de alimentação fornecem informações sobre o status do seu hardware, permitindo que você monitore possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e da trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Uma ou mais fontes de alimentação com falha(ocumEvtPowerSupplyOneOrMoreFailed)	Incidente	Nó	Crítico

Saiba mais sobre eventos de proteção no Active IQ Unified Manager

Os eventos de proteção informam se uma tarefa falhou ou foi abortada, para que você possa monitorar a ocorrência de 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 origem e a gravidade.

Área de impacto: proteção

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Tarefa de proteção falhou(ocumEvtProtectionJobTaskFailed)	Incidente	Serviço de volume ou armazenamento	Crítico
Tarefa de proteção abortada(ocumEvtProtectionJobAborted)	Risco	Serviço de volume ou armazenamento	Aviso

Saiba mais sobre eventos Qtree no Active IQ Unified Manager

Os eventos de qtree fornecem informações sobre a capacidade da qtree e os limites de arquivo e disco, permitindo que você monitore 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 origem e a gravidade.

Área de impacto: capacidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Espaço do qtree quase cheio(ocumEvtQtreeSpaceNearlyFull)	Risco	Qtree	Aviso
Espaço do qtree cheio(ocumEvtQtreeSpaceFull)	Risco	Qtree	Erro
Espaço do qtree normal(ocumEvtQtreeSpaceThresholdOk)	Evento	Qtree	Informação
Limite rígido de arquivos do qtree atingido(ocumEvtQtreeFilesHardLimitReached)	Incidente	Qtree	Crítico
Limite flexível de arquivos do qtree excedido(ocumEvtQtreeFilesSoftLimitBreached)	Risco	Qtree	Aviso
Limite rígido de espaço do qtree atingido(ocumEvtQtreeSpaceHardLimitReached)	Incidente	Qtree	Crítico
Limite flexível de espaço do qtree violado(ocumEvtQtreeSpaceSoftLimitBreached)	Risco	Qtree	Aviso

Saiba mais sobre os eventos do Service Processor no Active IQ Unified Manager

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, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Processador de serviço não configurado(ocumEvtServiceProcessorNotConfigured)	Risco	Nó	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Processador de serviço offline(ocumEvtServiceProcessorOffline)	Risco	Nó	Erro

Saiba mais sobre eventos de relação do SnapMirror no Active IQ Unified Manager

Os eventos de relação do SnapMirror fornecem informações sobre o status das suas relações assíncronas e síncronas do SnapMirror, para que você possa monitorar possíveis problemas. Os eventos de relação assíncrona do SnapMirror são gerados tanto para Storage VMs quanto para volumes, mas os eventos de relação síncrona do SnapMirror são gerados apenas para relações de volume. Não há eventos gerados para volumes constituintes que fazem parte de relações de recuperação de desastres de Storage VM. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: proteção

Um asterisco (*) identifica eventos do EMS que foram convertidos em eventos do Unified Manager.

> Os eventos de relacionamentos do SnapMirror são gerados para máquinas virtuais de armazenamento protegidas pela recuperação de desastres de máquina virtual de armazenamento, mas não para relacionamentos de objetos constituintes.

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Replicação espelhada não íntegra(ocumEvtSnapmirrorRelationshipUnhealthy)	Risco	Relação do SnapMirror	Aviso
Replicação de espelho interrompida(ocumEvtSnapmirrorRelationshipStateBrokenoff)	Risco	Relação do SnapMirror	Erro
Falha na inicialização da replicação de espelhamento (ocumEvtSnapmirrorRelationshipInitializeFailed)	Risco	Relação do SnapMirror	Erro
Falha na atualização da replicação do espelho(ocumEvtSnapmirrorRelationshipUpdateFailed)	Risco	Relação do SnapMirror	Erro

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Erro de atraso na replicação do espelho(ocumEvtSnapMirrorRelationshipLagError)	Risco	Relação do SnapMirror	Erro
Aviso de atraso na replicação de espelho(ocumEvtSnapMirrorRelationshipLagWarning)	Risco	Relação do SnapMirror	Aviso
Falha na ressincronização da replicação de espelho(ocumEvtSnapmirrorRelationshipResyncFailed)	Risco	Relação do SnapMirror	Erro
Replicação síncrona fora de sincronia *(syncSnapmirrorRelationshipOutofsync)	Risco	Relação do SnapMirror	Aviso
Replicação síncrona restaurada *(syncSnapmirrorRelationshipInSync)	Evento	Relação do SnapMirror	Informação
Falha na resincronização automática da replicação síncrona *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Risco	Relação do SnapMirror	Erro
O Ontap Mediator foi adicionado ao Cluster (snapmirrorMediatorAdded)	Evento	Cluster	Informação
O Ontap Mediator foi removido do Cluster (snapmirrorMediatorRemoved)	Evento	Cluster	Informação
O Ontap Mediator está inacessível a partir do cluster (snapmirrorMediatorUnreachable)	Risco	Mediator	Aviso
O Ontap Mediator não está acessível a partir do cluster (snapmirrorMediatorMisconfigured)	Risco	Mediator	Erro

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
A conectividade do Ontap Mediator foi restabelecida, está ressincronizada e pronta para a sincronização ativa do SnapMirror (snapmirrorMediatorInQuorum)	Evento	Mediator	Informação

Saiba mais sobre eventos de relação de espelhamento assíncrono e Vault no Active IQ Unified Manager

Os eventos de relacionamento do espelhamento assíncrono e do Vault fornecem a você informações sobre o status dos seus relacionamentos assíncronos do SnapMirror e do Vault para que você possa monitorar possíveis problemas. Os eventos de relacionamento do espelhamento assíncrono e do Vault são compatíveis com relacionamentos de proteção de volume e de Storage VM. Mas os relacionamentos somente do Vault não são compatíveis com a recuperação de desastres de Storage VM. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem e a severidade.

Área de impacto: proteção

Os eventos de relacionamentos do SnapMirror e do Vault também são gerados para VMs de armazenamento protegidas pela recuperação de desastres da VM de armazenamento, mas não para quaisquer relacionamentos de objetos constituintes.

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Espelho e Vault assíncronos não íntegros(ocumEvtMirrorVaultRelationshipUnhealthy)	Risco	Relação do SnapMirror	Aviso
Espelho assíncrono e Vault interrompidos(ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risco	Relação do SnapMirror	Erro
Falha na inicialização do espelho assíncrono e do cofre(ocumEvtMirrorVaultRelationshipInitializeFailed)	Risco	Relação do SnapMirror	Erro

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Falha na atualização assíncrona do espelho e do cofre(ocumEvtMirrorVaultRelationshipUpdateFailed)	Risco	Relação do SnapMirror	Erro
Erro de atraso do Mirror e Vault assíncronos(ocumEvtMirrorVaultRelationshipLagError)	Risco	Relação do SnapMirror	Erro
Aviso de atraso do espelhamento assíncrono e do Vault(ocumEvtMirrorVaultRelationshipLagWarning)	Risco	Relação do SnapMirror	Aviso
Falha na resincronização assíncrona do espelhamento e do cofre(ocumEvtMirrorVaultRelationshipResyncFailed)	Risco	Relação do SnapMirror	Erro

O evento "falha na atualização do SnapMirror" é gerado pelo portal Active IQ (Config Advisor).

Saiba mais sobre eventos de Snapshot no Active IQ Unified Manager

Os eventos de Snapshot fornecem informações sobre o status dos snapshots, permitindo que você os monitore 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 origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Exclusão automática de Snapshot desativada(não aplicável)	Evento	Volume	Informação
Exclusão automática de Snapshot ativada(não aplicável)	Evento	Volume	Informação
Configuração de exclusão automática de Snapshot modificada(não aplicável)	Evento	Volume	Informação

Saiba mais sobre eventos de relação do SnapVault no Active IQ Unified Manager

Os eventos de relação do SnapVault fornecem a você informações sobre o status das suas relações 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, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: proteção

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Vault assíncrono não íntegro(ocumEvtSnapVaultRelationshipUnhealthy)	Risco	Relação do SnapMirror	Aviso
SnapVault assíncrono interrompido(ocumEvtSnapVaultRelationshipStateBrokenoff)	Risco	Relação do SnapMirror	Erro
Falha na inicialização assíncrona do Vault(ocumEvtSnapVaultRelationshipInitializeFailed)	Risco	Relação do SnapMirror	Erro
Falha na atualização assíncrona do cofre(ocumEvtSnapVaultRelationshipUpdateFailed)	Risco	Relação do SnapMirror	Erro
Erro de atraso assíncrono do Vault(ocumEvtSnapVaultRelationshipLagError)	Risco	Relação do SnapMirror	Erro
Aviso de atraso assíncrono do Vault(ocumEvtSnapVaultRelationshipLagWarning)	Risco	Relação do SnapMirror	Aviso
Falha na resincronização assíncrona do Vault(ocumEvtSnapvaultRelationshipResyncFailed)	Risco	Relação do SnapMirror	Erro

Saiba mais sobre eventos de configurações de failover de armazenamento no Active IQ Unified Manager

Os eventos de configurações de failover de armazenamento (SFO) fornecem informações sobre se o failover de armazenamento está desativado ou não configurado para que você possa monitorar possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Interconexão de failover de armazenamento com um ou mais links inativos(ocumEvtSfoInterconnectOneOrMoreLinksDown)	Risco	Nó	Aviso
Failover de armazenamento desativado(ocumEvtSfoSettingsDisabled)	Risco	Nó	Erro
Failover de armazenamento não configurado(ocumEvtSfoSettingsNotConfigured)	Risco	Nó	Erro
Estado de failover de armazenamento - assumir o controle(ocumEvtSfoStateTakeover)	Risco	Nó	Aviso
Estado de failover de armazenamento - Retorno parcial(ocumEvtSfoStatePartialGiveback)	Risco	Nó	Erro
Status do nó de failover de armazenamento inativo(ocumEvtSfoNodeStatusDown)	Risco	Nó	Erro
O takeover do failover de armazenamento não é possível(ocumEvtSfoTakeoverNotPossible)	Risco	Nó	Erro

Saiba mais sobre eventos de serviços de armazenamento no Active IQ Unified Manager

Os eventos de serviços de armazenamento fornecem informações sobre a criação e a assinatura desses serviços, permitindo o monitoramento de possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: configuração

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Serviço de armazenamento criado(não aplicável)	Evento	Serviço de armazenamento	Informação
Serviço de armazenamento contratado(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 do trap)	Nível de impacto	Tipo de origem	Gravidade
Exclusão inesperada da relação gerenciada do SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion	Risco	Serviço de armazenamento	Aviso
Exclusão inesperada do volume do membro do serviço de armazenamento(ocumEvtStorageServiceUnexpectedVolumeDeletion)	Incidente	Serviço de armazenamento	Crítico

Saiba mais sobre eventos de armazenamento em prateleiras no Active IQ Unified Manager

Os eventos da gaveta de armazenamento informam se a sua gaveta de armazenamento apresenta alguma anormalidade, permitindo o monitoramento de 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 origem e a gravidade.

Área de impacto: disponibilidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Faixa de tensão anormal(ocumEvtShelfVoltageAbnormal)	Risco	Gaveta de armazenamento	Aviso
Faixa de corrente anormal(ocumEvtShelfCurrentAbnormal)	Risco	Gaveta de armazenamento	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Temperatura anormal(ocumEvtShelfTemperatureAbnormal)	Risco	Gaveta de armazenamento	Aviso

Saiba mais sobre eventos de VMs de armazenamento no Active IQ Unified Manager

Os eventos de máquina virtual de armazenamento (storage virtual machine, também conhecida como SVM) fornecem informações sobre o status das suas máquinas virtuais de armazenamento (SVMs), permitindo que você monitore possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem 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 do trap)	Nível de impacto	Tipo de origem	Gravidade
Serviço CIFS da VM de storage inativo(ocumEvtVserverCifsServiceStatusDown)	Incidente	SVM	Crítico
Serviço CIFS da SVM não configurado(não aplicável)	Evento	SVM	Informação
Tentativas de conexão a compartilhamento CIFS inexistente *(nbladeCifsNoPrivShare)	Incidente	SVM	Crítico
Conflito de nome NetBIOS do CIFS *(nbladeCifsNbNameConflict)	Risco	SVM	Erro
Falha na operação de cópia de sombra do CIFS *(cifsShadowCopyFailure)	Risco	SVM	Erro
Muitas conexões CIFS *(nbladeCifsManyAuths)	Risco	SVM	Erro
Número máximo de conexões CIFS excedido *(nbladeCifsMaxOpenSameFile)	Risco	SVM	Erro

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Número máximo de conexões CIFS por usuário excedido *(nbladeCifsMaxSessPerUsrConn)	Risco	SVM	Erro
Serviço FC/FCoE da SVM inativo(ocumEvtVserverFcServiceStatusDown)	Incidente	SVM	Crítico
Serviço iSCSI da SVM inativo(ocumEvtVserverIscsiServiceStatusDown)	Incidente	SVM	Crítico
Serviço NFS da VM de storage inativo (ocumEvtVserverNfsServiceStatusDown)	Incidente	SVM	Crítico
Serviço SVM FC/FCoE não configurado(não aplicável)	Evento	SVM	Informação
Serviço iSCSI da SVM não configurado(não aplicável)	Evento	SVM	Informação
Serviço NFS do SVM não configurado (não aplicável)	Evento	SVM	Informação
Máquina virtual 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 do trap)	Nível de impacto	Tipo de origem	Gravidade
Sem conexão responsiva com o servidor AV *(nbladeVscanConnInactive)	Evento	SVM	Informação
Tentativa de usuário não autorizado de acessar o servidor AV *(nbladeVscanBadUserPrivAccess)	Risco	SVM	Erro
Vírus detectado pelo servidor antivírus *(nbladeVscanVirusDetected)	Risco	SVM	Erro

Área de impacto: configuração

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
SVM detectado(Não aplicável)	Evento	SVM	Informação
SVM excluído(não aplicável)	Evento	Cluster	Informação
SVM renomeado(não aplicável)	Evento	SVM	Informação

Área de impacto: desempenho

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limiar crítico de IOPS do SVM ultrapassado(ocumSvmIopsIncident)	Incidente	SVM	Crítico
Limiar de aviso de IOPS do SVM ultrapassado(ocumSvmIopsWarning)	Risco	SVM	Aviso
Limiar crítico de MB/s do SVM ultrapassado(ocumSvmMbpsIncident)	Incidente	SVM	Crítico
Limiar de aviso de MB/s da SVM ultrapassado(ocumSvmMbpsWarning)	Risco	SVM	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limiar crítico de latência da SVM ultrapassado(ocumSvmLatencyIncident)	Incidente	SVM	Crítico
Limiar de aviso de latência do SVM ultrapassado(ocumSvmLatencyWarning)	Risco	SVM	Aviso

Área de impacto: segurança

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Registro de auditoria desativado(ocumVserverAuditLogDisabled)	Risco	SVM	Aviso
Banner de login desativado(ocumVserverLoginBannerDisabled)	Risco	SVM	Aviso
O 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 desativado (antiRansomwareSvmStateDisabled)	Risco	SVM	Aviso
O monitoramento antiransomware da VM de storage está ativado (modo de aprendizado) (antiRansomwareSvmStateDryrun)	Evento	SVM	Informação
Máquina virtual de storage adequada para monitoramento anti-ransomware (Modo de Aprendizagem) (ocumEvtSvmArwCandidate)	Evento	SVM	Informação

Saiba mais sobre eventos de cotas de usuário e grupo no Active IQ Unified Manager

Os eventos de cota de usuário e grupo fornecem informações sobre a capacidade da cota do usuário e do 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 do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: capacidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Cota de espaço em disco do usuário ou grupo Limite flexível atingido(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risco	Cota de usuário ou grupo	Aviso
Limite máximo de espaço em disco da cota de usuário ou grupo atingido(ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Incidente	Cota de usuário ou grupo	Crítico
Limite flexível de contagem de arquivos da cota de usuário ou grupo excedido(ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Risco	Cota de usuário ou grupo	Aviso
Limite rígido de contagem de arquivos da cota de usuário ou grupo atingido(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Incidente	Cota de usuário ou grupo	Crítico

Saiba mais sobre eventos de volume no Active IQ Unified Manager

Os eventos de volume fornecem informações sobre o status dos volumes, permitindo que você monitore 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 origem 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 do trap)	Nível de impacto	Tipo de origem	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
Volume remontado(não aplicável)	Evento	Volume	Informação
Caminho de junção de volume inativo(ocumEvtVolumeJunctionPathInactive)	Risco	Volume	Aviso
Dimensionamento automático de volume ativado(não aplicável)	Evento	Volume	Informação
Autodimensionamento de volume desativado(não aplicável)	Evento	Volume	Informação
Volume Autosize Capacidade Máxima Modificada(Não aplicável)	Evento	Volume	Informação
Tamanho do incremento do dimensionamento automático do volume modificado(não aplicável)	Evento	Volume	Informação

Área de impacto: capacidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Espaço de volume provisionado dinamicamente em risco(ocumThinProvisionVolumeSpaceAtRisk)	Risco	Volume	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Erro de operação de eficiência de volume(ocumEvtVolumeEfficiencyOperationError)	Risco	Volume	Erro
Espaço de volume cheio(ocumEvtVolumeFull)	Risco	Volume	Erro
Espaço do volume quase cheio(ocumEvtVolumeNearlyFull)	Risco	Volume	Aviso
Espaço Lógico do Volume Cheio *(volumeLogicalSpaceFull)	Risco	Volume	Erro
Espaço lógico do volume quase cheio *(volumeLogicalSpaceNearlyFull)	Risco	Volume	Aviso
Espaço lógico do volume normal *(volumeLogicalSpaceAllOK)	Evento	Volume	Informação
Espaço de reserva do Snapshot do volume cheio(ocumEvtSnapshotFull)	Risco	Volume	Aviso
Muitas cópias Snapshot(ocumEvtSnapshotTooMany)	Risco	Volume	Erro
Cota de qtree de volume com excesso de provisionamento (ocumEvtVolumeQtreeQuotaOvercommitted)	Risco	Volume	Erro
Quota de qtree do volume quase supercomprometida(ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Risco	Volume	Aviso
Taxa de crescimento de volume anormal(ocumEvtVolumeGrowthRateAbnormal)	Risco	Volume	Aviso
Dias até o volume encher(ocumEvtVolumeDaysUntilFullSoon)	Risco	Volume	Erro

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Garantia de espaço do volume desativada(não aplicável)	Evento	Volume	Informação
Garantia de espaço do volume ativada(não aplicável)	Evento	Volume	Informação
Garantia de espaço do volume modificada(não aplicável)	Evento	Volume	Informação
Reserva de Snapshot do volume: dias até atingir a capacidade máxima(ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risco	Volume	Erro
FlexGroup Constituintes com problemas de espaço *(flexGroupConstituentsHaveSpaceIssues)	Risco	Volume	Erro
FlexGroup status do espaço dos constituintes tudo OK *(flexGroupConstituentsSpaceStatusAllOK)	Evento	Volume	Informação
FlexGroup Constituintes têm problemas com inodes *(flexGroupConstituentsHaveInodesIssues)	Risco	Volume	Erro
FlexGroup Status dos inodes dos constituintes: todos OK *(flexGroupConstituentsInodesStatusAllOK)	Evento	Volume	Informação
Volume WAFL AutoSize com falha *(waflVolAutoSizeFail)	Risco	Volume	Erro
WAFL Volume AutoSize concluído *(waflVolAutoSizeDone)	Evento	Volume	Informação
FlexGroup volume está com mais de 80% de utilização*	Incidente	Volume	Erro

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
FlexGroup volume está com mais de 90% de utilização*	Incidente	Volume	Crítico
Anomalia na eficiência de storage do volume (ocumVolumeAbnormalStorageEfficiencyWarning)	Risco	Volume	Aviso
Reserva de Snapshot do volume subutilizada (volumeSnaphotReserveUnderutilizedWarning)	Evento	Volume	Aviso
Reserva de Snapshot do volume subutilizada (volumeSnaphotReserveUnderutilizedCleared)	Evento	Volume	Aviso

Área de impacto: configuração

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Volume renomeado(Não aplicável)	Evento	Volume	Informação
Volume descoberto(não aplicável)	Evento	Volume	Informação
Volume excluído(Não aplicável)	Evento	Volume	Informação

Área de impacto: desempenho

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limiar de aviso de IOPS máximo de volume QoS ultrapassado(ocumQosVolumeMaxIopsWarning)	Risco	Volume	Aviso
Limiar de aviso de MB/s máx. do volume QoS excedido(ocumQosVolumeMaxMbpsWarning)	Risco	Volume	Aviso
Limiar de aviso de IOPS/TB máximas do volume de QoS ultrapassado(ocumQosVolumeMaxIopsPerTbWarning)	Risco	Volume	Aviso

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limite de latência do volume de carga de trabalho excedido conforme definido pela política de nível de serviço de desempenho(ocumConformanceLatencyWarning)	Risco	Volume	Aviso
Limite crítico de IOPS do volume excedido(ocumVolumeIopsIncident)	Incidente	Volume	Crítico
Limiar de aviso de IOPS de volume ultrapassado(ocumVolumeIopsWarning)	Risco	Volume	Aviso
Limiar crítico de MB/s do volume ultrapassado(ocumVolumeMbpsIncident)	Incidente	Volume	Crítico
Limite de aviso de MB/s do volume ultrapassado(ocumVolumeMbpsWarning)	Risco	Volume	Aviso
Limiar crítico de latência de volume ultrapassado(ocumVolumeLatencyIncident)	Incidente	Volume	Crítico
Limite de aviso de latência do volume excedido(ocumVolumeLatencyWarning)	Risco	Volume	Aviso
Limite crítico da taxa de falhas de cache do volume ultrapassado(ocumVolumeCacheMissRatioIncident)	Incidente	Volume	Crítico
Limiar de aviso de taxa de falhas de cache de volume ultrapassado(ocumVolumeCacheMissRatioWarning)	Risco	Volume	Aviso
Limiar crítico de latência de volume e IOPS ultrapassado(ocumVolumeLatencyIopsIncident)	Incidente	Volume	Crítico

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Limiar de aviso de latência de volume e IOPS ultrapassado(ocumVolumeLatencyIopsWarning)	Risco	Volume	Aviso
Latência de volume e limite crítico de MB/s ultrapassado(ocumVolumeLatencyMbpsIncident)	Incidente	Volume	Crítico
Latência do volume e limite de aviso de MB/s ultrapassado(ocumVolumeLatencyMbpsWarning)	Risco	Volume	Aviso
Latência do volume e limite crítico de capacidade de desempenho do agregado usado violado(ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Incidente	Volume	Crítico
Latência do volume e limite de aviso de capacidade de desempenho do agregado usado ultrapassado(ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Risco	Volume	Aviso
Limiar crítico de latência do volume e utilização do agregado ultrapassado(ocumVolumeLatencyAggregateUtilizationIncident)	Incidente	Volume	Crítico
Limite de aviso de latência de volume e utilização de agregado ultrapassado(ocumVolumeLatencyAggregateUtilizationWarning)	Risco	Volume	Aviso
Violação do limite crítico de latência do volume e capacidade de desempenho do nó usada(ocumVolumeLatencyNodePerfCapacityUsedIncident)	Incidente	Volume	Crítico

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Latência do volume e limite de aviso de capacidade de desempenho do nó usada violado(ocumVolumeLatencyNodePerfCapacityUsedWarning)	Risco	Volume	Aviso
Latência do volume e capacidade de desempenho do nó usada - limite crítico de tomada de controle ultrapassado(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incidente	Volume	Crítico
Latência de volume e capacidade de desempenho do nó utilizada: limite de aviso de takeover ultrapassado(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risco	Volume	Aviso
Limiar crítico de latência do volume e utilização do nó ultrapassado(ocumVolumeLatencyNodeUtilizationIncident)	Incidente	Volume	Crítico
Limite de aviso de latência de volume e utilização do nó ultrapassado(ocumVolumeLatencyNodeUtilizationWarning)	Risco	Volume	Aviso

Área de impacto: segurança

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
O monitoramento antirransomware do volume está ativado (modo ativo) (antiRansomwareVolumeStateEnabled)	Evento	Volume	Informação

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
O monitoramento de volume contra ransomware está desativado (antiRansomwareVolumeStateDisabled)	Risco	Volume	Aviso
O monitoramento anti-ransomware do volume está ativado (modo de aprendizado) (antiRansomwareVolumeStateDryrun)	Evento	Volume	Informação
O monitoramento anti-ransomware do volume está pausado (modo de aprendizado) (antiRansomwareVolumeStateDryrunPaused)	Risco	Volume	Aviso
O monitoramento anti-ransomware do volume está pausado (modo ativo) (antiRansomwareVolumeStateEnablePaused)	Risco	Volume	Aviso
O monitoramento de volume anti-ransomware está sendo desativado (antiRansomwareVolumeStateDisableInProgress)	Risco	Volume	Aviso
Atividade de ransomware detectada (callHomeRansomwareActivitySeen)	Incidente	Volume	Crítico
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

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
O volume exibe alertas anti-ransomware ruidosos (antiRansomwareFeature NoisyVolume)	Risco	Volume	Aviso

Área de impacto: proteção de dados

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
O volume tem proteção local de Snapshot insuficiente (volumeLacksLocalProtectionWarning)	Risco	Volume	Aviso
O volume não tem proteção local de Snapshot suficiente (volumeLacksLocalProtectionCleared)	Risco	Volume	Aviso

Saiba mais sobre eventos de status de movimentação de volume no Active IQ Unified Manager

Os eventos de status de movimentação de volume informam sobre o status da sua movimentação de volume, permitindo que você monitore possíveis problemas. Os eventos são agrupados por área de impacto e incluem o nome do evento e do trap, o nível de impacto, o tipo de origem e a gravidade.

Área de impacto: capacidade

Nome do evento (Nome do trap)	Nível de impacto	Tipo de origem	Gravidade
Status da movimentação de volume: em andamento(não aplicável)	Evento	Volume	Informação
Status da movimentação de volume - Falha(ocumEvtVolumeMoveFailed)	Risco	Volume	Erro
Status da movimentação de volume: concluída(não aplicável)	Evento	Volume	Informação
Movimentação de Volume - Transição Adiada(ocumEvtVolumeMoveCutoverDeferred)	Risco	Volume	Aviso

Descrição das janelas de eventos e caixas de diálogo

Saiba mais sobre a página de Notificações em o Active IQ Unified Manager

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, as notificações podem ser enviadas como e-mails ou traps SNMP.

Você precisa ter a função de Application Administrator ou Storage Administrator.

E-mail

Esta área permite que você configure as seguintes configurações de email para notificação de alerta:

- **Endereço do remetente**

  Especifica o endereço de e-mail do qual a notificação de alerta é enviada. Esse valor também é usado como endereço de remetente de um relatório quando ele é compartilhado. Se o endereço de remetente estiver preenchido automaticamente com "ActiveIQUnifiedManager@localhost.com", você deve alterá-lo para um endereço de e-mail real e válido para garantir que todas as notificações por e-mail sejam entregues com sucesso.

Servidor SMTP

Esta área permite configurar as seguintes definições do servidor SMTP:

- **Nome do host ou endereço IP**

  Especifica o nome do host do seu servidor SMTP, que será 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 apenas quando o SMTPAUTH está habilitado no servidor SMTP.

- **Senha**

  Especifica a senha SMTP. O nome de usuário SMTP é necessário apenas 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.

- **Usar START/TLS**

  Marcar esta caixa permite a comunicação segura entre o servidor SMTP e o servidor de gerenciamento utilizando os protocolos TLS/SSL (também conhecidos como start_tls e StartTLS).

- **Usar SSL**

Marcar esta caixa permite a comunicação segura entre o servidor SMTP e o servidor de gerenciamento utilizando o protocolo SSL.

SNMP

Esta área permite configurar as seguintes configurações de trap SNMP:

- **Versão**

  Especifica a versão SNMP que você deseja usar, dependendo do tipo de segurança necessário. As opções incluem Versão 1, Versão 3, Versão 3 com Autenticação e Versão 3 com Autenticação e Criptografia. O valor padrão é Versão 1.

- **Host de destino da trap**

  Especifica o nome do host ou endereço IP (IPv4 ou IPv6) que receberá os traps SNMP enviados pelo servidor de gerenciamento. Para especificar vários destinos de trap, separe cada host com uma vírgula.

  > Todas as outras configurações SNMP, como "Versão" e "Porta de saída", devem ser as mesmas para todos os hosts da lista.

- **Porta de trap de saída**

  Especifica a porta através da qual o servidor SNMP recebe os traps enviados pelo servidor de gerenciamento.

  O valor padrão é 162.

- **Comunidade**

  A string de comunidade para acessar o host.

- **ID do mecanismo**

  Especifica o identificador exclusivo do agente SNMP e é gerado automaticamente pelo servidor de gerenciamento. O Engine ID está disponível com SNMP Version 3, SNMP Version 3 with Authentication e SNMP Version 3 with Authentication and Encryption.

- **Nome de usuário**

  Especifica o nome de usuário SNMP. O nome de usuário está disponível na versão 3 do SNMP, na versão 3 do SNMP com autenticação e na versão 3 do SNMP 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 no SNMP versão 3 com autenticação e no 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 na versão 3 do SNMP com autenticação e criptografia.

- **Senha de privacidade**

  Especifica a senha ao usar o protocolo de privacidade. A senha de privacidade está disponível com a versão 3 do SNMP com autenticação e criptografia.

Para obter mais informações sobre objetos e traps SNMP, você pode baixar o "MIB do Active IQ Unified Manager" no site de suporte da NetApp.

Saiba mais sobre a página de inventário de Gerenciamento de Eventos no Active IQ Unified Manager

A página de inventário do Gerenciamento de Eventos permite que você visualize uma lista dos eventos atuais e suas propriedades. Você pode realizar tarefas como reconhecer, resolver e atribuir eventos. Você também pode adicionar um alerta para eventos específicos.

As informações desta página são atualizadas automaticamente a cada 5 minutos para garantir que os eventos novos mais recentes sejam exibidos.

Componentes do filtro

Permite personalizar as informações exibidas na lista de eventos. Você pode refinar a lista de eventos exibida usando os seguintes componentes:

- Menu Exibir para selecionar em uma lista predefinida de filtros.

  Isso inclui itens como todos os eventos ativos (novos e confirmados), 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.
- O botão Filtrar abre o painel Filtros para que você selecione entre 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 selecionar o usuário ao qual o evento será atribuído. Ao atribuir um evento a um usuário, a lista de eventos dos eventos selecionados passa a exibir o nome do usuário e a hora em que você atribuiu o evento.

  - Eu

    Atribui o evento ao usuário atualmente conectado.

  - Outro usuário

    Exibe a caixa de diálogo Atribuir proprietário, que permite atribuir ou reatribuir o evento a outros

usuários. Você também pode remover 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 dos eventos selecionados. Quando você reconhece um evento, você passa a ser responsável por gerenciá-lo.

  Não é possível confirmar eventos de informação.

- **Marcar como resolvido**

  Permite que você altere o estado do evento para resolvido.

  Ao resolver um evento, seu nome de usuário e a hora em que você resolveu o evento são adicionados à lista de eventos para os eventos selecionados. Após tomar as medidas corretivas necessárias para o evento, você deve marcar o evento como resolvido.

- **Adicionar alerta**

  Exibe a caixa de diálogo Adicionar Alerta, que permite adicionar alertas para os eventos selecionados.

- **Relatórios**

  Permite que você exporte os detalhes da visualização atual de eventos para um arquivo de valores separados por vírgula (.csv) ou documento PDF.

- **Mostrar/Ocultar Seletor de Colunas**

  Permite escolher as colunas que serão exibidas na página e selecionar a ordem em que serão apresentadas.

Lista de eventos

Exibe detalhes de todos os eventos ordenados por horário de disparo.

Por padrão, a visualização "Todos os eventos ativos" é exibida para mostrar os eventos novos e reconhecidos dos sete dias anteriores que têm um nível de impacto de incidente ou risco.

- **Hora de acionamento**

  O momento em que o evento foi gerado.

- **Gravidade**

  A gravidade do evento: crítico ( ), erro ( ), aviso ( ) e informação ( ).

- **Estado**

  Estado do evento: novo, reconhecido, resolvido ou obsoleto.

- **Nível de impacto**

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 de detalhes do evento para esse evento.

- **Fonte**

  O nome do objeto no qual o evento ocorreu. Você pode selecionar o nome para exibir a página de detalhes de integridade ou desempenho desse objeto.

  Quando ocorre uma violação da política de QoS compartilhada, apenas o objeto de carga de trabalho que está consumindo mais IOPS ou MB/s é exibido neste campo. Cargas de trabalho adicionais que utilizam essa política são exibidas na página de 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 está atribuído.

- **Origem do evento**

  Se o evento se originou 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 anotações adicionadas a um evento.

- **Dias Pendentes**

  O número de dias desde que o evento foi gerado inicialmente.

- **Horário atribuído**

  O tempo decorrido desde que o evento foi atribuído a um usuário. Se o tempo decorrido for superior a uma semana, será exibido o carimbo de data e hora em que o evento foi atribuído a um usuário.

- **Confirmado por**

  Nome do usuário que confirmou o evento. O campo fica em branco se o evento não for confirmado.

- **Hora de reconhecimento**

O tempo decorrido desde que o evento foi reconhecido. Se o tempo decorrido for superior a uma semana, será exibido o horário em que o evento foi reconhecido.

- **Resolvido por**

  O nome do usuário que resolveu o evento. O campo fica em branco se o evento não estiver resolvido.

- **Horário de resolução**

  O tempo decorrido desde que o evento foi resolvido. Se o tempo decorrido exceder uma semana, será exibido o carimbo de data e hora em que o evento foi resolvido.

- **Tempo obsoleto**

  O momento em que o estado do evento se tornou Obsolete.

Página de detalhes do evento

Saiba mais sobre a página de detalhes do evento no Active IQ Unified Manager

Na página de detalhes do evento, você pode visualizar os detalhes de um evento selecionado, como a gravidade do evento, o nível de impacto, a área de impacto e a 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 apareceu pela última vez.

  Para eventos que não sejam de desempenho, enquanto o evento estiver no estado Novo ou Reconhecido, as informações sobre a última ocorrência não são conhecidas e, portanto, ficam ocultas.

- **Descrição do evento**

  Uma breve descrição do evento.

  Em alguns casos, a descrição do evento informa o motivo pelo qual o evento foi acionado.

- **Componente em Disputa**

  Para eventos de desempenho dinâmico, esta seção exibe ícones que representam os componentes lógicos e físicos do cluster. Se um componente estiver em contenção, seu ícone aparecerá circulado e destacado em vermelho.

  Consulte *Componentes do cluster e por que eles podem estar em contenção* para obter uma descrição dos componentes exibidos aqui.

As seções Informações sobre o 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

- **Atribua-me**

  Atribui o evento a você.

- **Atribuir a outros**

  Abre a caixa de diálogo Assign Owner, que permite que você atribua ou reatribua o evento a outros usuários.

  Ao atribuir um evento a um usuário, o nome do usuário e a hora em que o evento foi atribuído são adicionados à lista de eventos para os eventos selecionados.

  Você também pode remover 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.

  Ao reconhecer 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. Ao reconhecer um evento, você assume a responsabilidade por gerenciar esse evento.

- **Marcar como resolvido**

  Permite alterar o estado do evento para Resolvido.

  Ao resolver um evento, seu nome de usuário e a hora em que você resolveu o evento são adicionados à lista de eventos (Resolvido por) para os eventos selecionados. Após tomar as medidas corretivas necessárias 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.

Saiba mais sobre a seção Informações do Evento no Active IQ Unified Manager

Na página de detalhes do evento, você usa a seção Informações do Evento para ver os detalhes sobre um evento selecionado, como a gravidade do evento, o nível de impacto, a área de impacto e a origem do evento.

Os campos que não se aplicam ao tipo de evento estão ocultos. Você pode visualizar os seguintes detalhes do evento:

- **Tempo de disparo do evento**

  O momento em que o evento foi gerado.

- **Estado**

  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 decorrido entre a detecção e a última análise do evento. Para eventos obsoletos, este é o tempo decorrido 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 após terem sido resolvidos ou se tornado 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 do que o horário 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 estiverem no estado Novo ou Reconhecido, esse conteúdo não é atualizado e, portanto, o campo fica oculto.

- **Gravidade**

  A gravidade do evento: crítico (), erro (), aviso () e informação ().

- **Nível de impacto**

  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, este campo lista até três dos objetos de carga de trabalho que consomem mais IOPS ou MBps.

  Você pode clicar no link do nome da fonte para exibir a página de detalhes de integridade ou desempenho desse objeto.

- **Anotações de origem**

  Exibe o nome e o valor da anotação do objeto ao qual o evento está associado.

  Este campo é exibido apenas para eventos de integridade em clusters, SVMs e volumes.

- **Grupos de origem**

Exibe os nomes de todos os grupos aos quais o objeto afetado pertence.

Este campo é exibido apenas para eventos de integridade em clusters, SVMs e volumes.

- **Tipo de fonte**

  O tipo de objeto (por exemplo, SVM, Volume ou Qtree) ao qual o evento está associado.

- **No Cluster**

  O nome do cluster no qual o evento ocorreu.

  Você pode clicar no link do nome do cluster para exibir a página com detalhes de integridade ou desempenho desse cluster.

- **Número de objetos afetados**

  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 apenas para eventos de desempenho.

- **Volumes afetados**

  O número de volumes que estão sendo afetados por este evento.

  Este campo é exibido apenas para eventos de desempenho em nós ou agregados.

- **Política acionada**

  O nome da política de limite que gerou o evento.

  Você pode posicionar o cursor sobre o nome da política para ver os detalhes da política de limite. Para políticas de QoS adaptável, a política definida, o tamanho do bloco e o tipo de alocação (espaço alocado ou espaço usado) também são exibidos.

  Este campo é exibido apenas para eventos de desempenho.

- **ID da regra**

  Para eventos da plataforma Active IQ, este é o número da regra acionada para gerar o evento.

- **Reconhecido por**

  O nome da pessoa que reconheceu o evento e o horário em que o evento foi reconhecido.

- **Resolvido por**

  O nome da pessoa que resolveu o evento e o horário 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:

  - Caso não haja alertas associados ao evento selecionado, você verá um link **Adicionar alerta**.

    Você pode abrir a caixa de diálogo Adicionar Alerta clicando no link.

  - Se houver um alerta associado ao evento selecionado, o nome do alerta é 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 é exibido.

    Você pode acessar a página de Configuração de Alertas clicando no link para visualizar mais detalhes sobre esses alertas.

  Os alertas desativados não são exibidos.

- **Última notificação enviada**

  A data e a hora em que a notificação de alerta mais recente foi enviada.

- **Enviar por**

  O mecanismo utilizado para enviar a notificação de alerta foi: e-mail ou SNMP trap.

- **Execução de script anterior**

  O nome do script executado quando o alerta foi gerado.

Saiba mais sobre as ações sugeridas no Active IQ Unified Manager

A seção Ações sugeridas da página de detalhes do evento fornece possíveis causas para o evento e sugere algumas ações para que você possa tentar resolvê-lo por conta própria. As ações sugeridas são personalizadas com base no tipo de evento ou no tipo de limite que foi ultrapassado.

Esta área é exibida apenas para alguns tipos de eventos.

Em alguns casos, há links de **Ajuda** fornecidos na página que remetem 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, de comandos da CLI do ONTAP ou de uma combinação dessas ferramentas.

Você deve considerar as ações sugeridas aqui apenas como uma orientação para resolver este evento. A ação que você tomar para resolver este evento deve se basear no contexto do seu ambiente.

Se você deseja analisar o objeto e o evento com mais detalhes, clique no botão **Analisar Carga de Trabalho** para exibir a página de Análise de Carga de Trabalho.

Há certos eventos que o Unified Manager pode diagnosticar minuciosamente e fornecer uma única solução. Quando disponíveis, essas soluções são exibidas com um botão **Fix It**. Clique neste botão para que o Unified Manager corrija o problema que causou o evento.

Para eventos de plataforma do 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 externo à rede, 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.

Saiba mais sobre o diagnóstico do sistema no Active IQ Unified Manager

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 mais afetam a latência ou são mais 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, bully ou shark no componente em contenção.
- Atividade da carga de trabalho: exibe detalhes sobre o uso da carga de trabalho do componente do cluster em contenção.
- Atividade de recursos: exibe estatísticas históricas de desempenho para o componente do cluster em contenção.

Outros gráficos são exibidos quando alguns componentes do cluster estão em contenção.

Outros eventos fornecem uma breve descrição do tipo de análise que o sistema está realizando no objeto de armazenamento. Em alguns casos, haverá uma ou mais linhas, uma para cada componente analisado, para políticas de desempenho definidas pelo sistema que analisam vários contadores de desempenho. 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.

Saiba mais sobre a página de Configuração de Eventos no Active IQ Unified Manager

A página Configuração de Eventos exibe a lista de eventos desativados e fornece informações como o tipo de objeto associado e a gravidade do evento. Você também pode executar tarefas como desativar ou ativar eventos globalmente.

Você só pode 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**

  Abre a caixa de diálogo Disable Events, que você pode usar para desativar eventos.

- **Habilitar**

Ativa os eventos selecionados que você havia optado por desativar anteriormente.

- **Regras de Upload**

  Abre a caixa de diálogo "Regras de upload", que permite que sites sem acesso externo à rede carreguem manualmente o arquivo de regras do Active IQ para o Unified Manager. As regras são executadas nas mensagens do cluster AutoSupport para gerar eventos de configuração do sistema, cabeamento, melhores práticas e disponibilidade, conforme definido pela plataforma Active IQ.

- **Inscreva-se nos eventos de EMS**

  Abre a caixa de diálogo "Inscrever-se em eventos do EMS", que permite que você se inscreva para receber eventos específicos do Event Management System (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 do EMS assinado, um evento do Unified Manager é gerado com a severidade apropriada.

Visualização em lista

A visualização em lista exibe (em formato tabular) informações sobre eventos desativados. Você pode usar os filtros de coluna para personalizar os dados exibidos.

- **Evento**

  Exibe o nome do evento que está desativado.

- **Gravidade**

  Exibe a gravidade do evento. A gravidade pode ser Crítica, Erro, Aviso ou Informação.

- **Tipo de fonte**

  Exibe o tipo de origem para o qual o evento é gerado.

Desative a caixa de diálogo Eventos no Active IQ Unified Manager

A caixa de diálogo Disable Events exibe a lista de tipos de evento para os quais você pode desativar eventos. Você pode desativar eventos para um tipo de evento com base em uma gravidade específica ou para um conjunto de eventos.

Você precisa ter a função de Application Administrator ou Storage Administrator.

Área de propriedades do evento

A área Propriedades do evento especifica as seguintes propriedades do evento:

- **Gravidade do evento**

  Permite que você selecione eventos com base no tipo de gravidade, que pode ser Crítico, Erro, Aviso ou Informação.

- **O nome do evento contém**

  Permite que você filtre eventos cujos nomes contenham os caracteres especificados.

- **Eventos correspondentes**

  Exibe a lista de eventos que correspondem ao tipo de gravidade e à cadeia de texto que você especificar.

- **Desativar eventos**

  Exibe a lista de eventos que você selecionou para desativar.

  A gravidade do evento também é exibida juntamente com o nome do evento.

Botões de comando

Os botões de comando permitem 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

Saiba mais sobre alertas no Active IQ Unified Manager

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 executado quando um alerta é acionado.

Os critérios de filtro incluem classe do objeto, nome ou gravidade do evento.

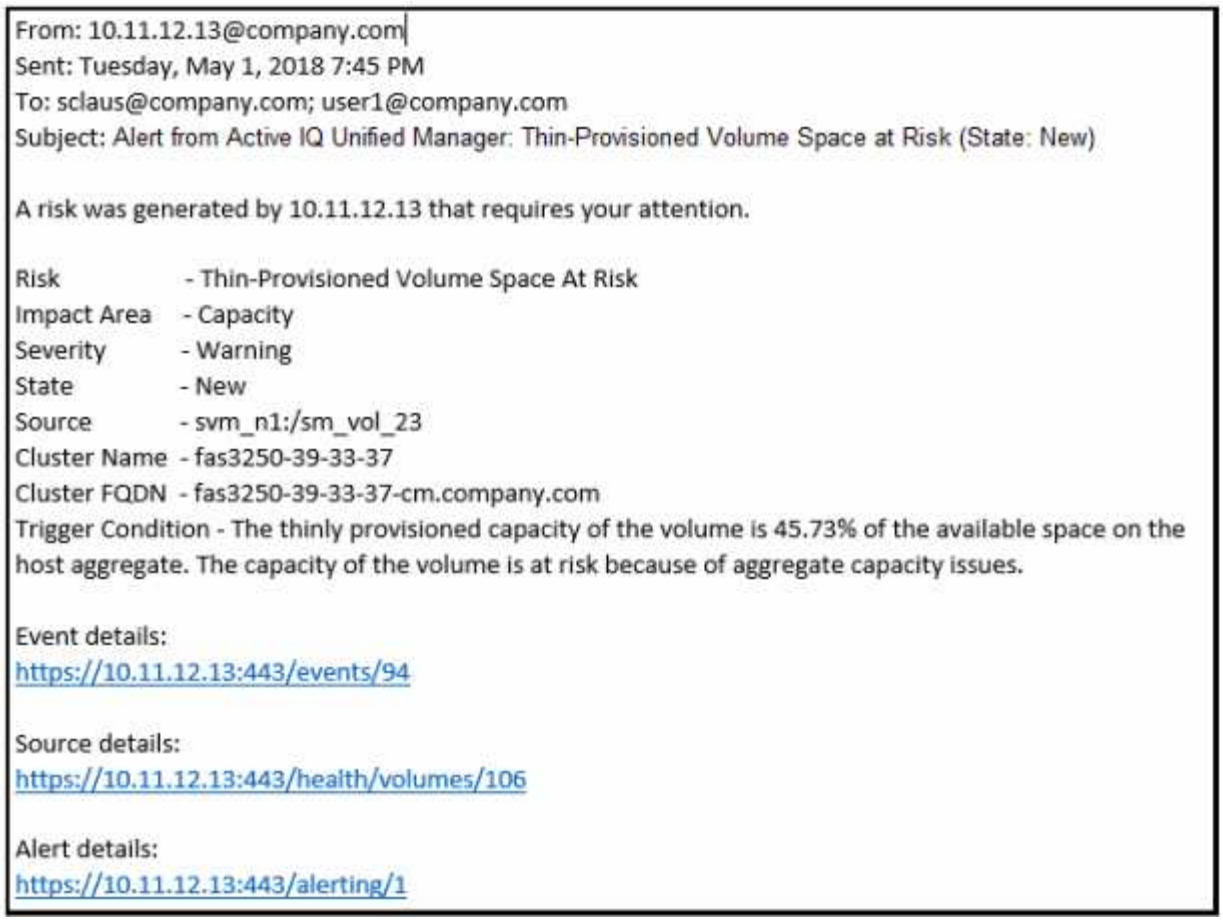
Informações contidas em um e-mail de alerta do Active IQ Unified Manager

Os e-mails de alerta do Unified Manager fornecem o tipo de evento, a gravidade do evento, o nome da política ou do limite que foi violado e causou o evento, além de uma descrição do evento. A mensagem de e-mail também inclui um hiperlink para cada evento, permitindo que você visualize a página de detalhes do evento na interface do usuário.

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

Se um contador de desempenho ou um valor de capacidade sofrer uma grande alteração durante um período de coleta, isso poderá acionar simultaneamente um evento crítico e um evento de aviso para a mesma política de limite. Nesse caso, você poderá receber um e-mail para o evento de aviso e outro para o evento crítico. Isso ocorre porque o Unified Manager permite que você se inscreva separadamente para receber alertas de violações de limite de aviso e crítico.

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



Adicionar alertas

Adicione alertas no Active IQ Unified Manager

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

Antes de começar

- Você precisa ter configurado as definições de notificação, como o endereço de e-mail do usuário, o servidor SMTP e o host de trap SNMP, para permitir que o servidor Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento for gerado.
- Você precisa saber os recursos e eventos para os quais deseja acionar o alerta, bem como os nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se você quiser que um script seja executado com base no evento, deve ter adicionado o script ao Unified Manager usando a página Scripts.
- Você precisa ter a função de Application Administrator ou Storage Administrator.

Além de criar um alerta na página de Configuração de Alertas, conforme descrito aqui, você pode criá-lo diretamente na página de detalhes do evento após receber um evento.

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de**

alertas.

2. Na página **Alert Setup**, clique em **Add**.
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 que deseja incluir ou excluir do alerta.

   Você pode definir um filtro especificando uma cadeia de texto no campo **Nome contém** para selecionar um grupo de recursos. Com base na cadeia de texto que você especificar, a lista de recursos disponíveis exibe apenas os recursos que correspondem à regra de filtro. A cadeia de texto que você especificar diferencia maiúsculas de minúsculas.

   Se um recurso estiver em conformidade com as regras de inclusão e exclusão que você especificou, a regra de exclusão tem precedência sobre a regra de inclusão, e o alerta não é gerado para eventos relacionados ao recurso excluído.

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

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

6. Clique em **Ações** e selecione os usuários que você deseja notificar, escolha a frequência de notificação, defina se um trap SNMP será enviado ao receptor de traps e atribua um script para executar 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, pois o endereço de e-mail modificado não estará mais vinculado ao 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 como adicionar um alerta

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

- Nome do alerta: HealthTest
- Recursos: inclui todos os volumes cujos nomes contêm "abc" e exclui todos os volumes cujos nomes contêm "xyz"
- Eventos: inclui todos os eventos críticos de saúde
- Ações: inclui "sample@domain.com", um script "Test" e o usuário deve ser notificado a cada 15 minutos

Execute as etapas a seguir na caixa de diálogo Add Alert:

1. Clique em **Nome** e digite **`HealthTest`** no campo **Nome do alerta**.
2. Clique em **Resources** e, na guia Include, selecione **Volumes** na lista suspensa.
   a. Digite **`abc`** no campo **Nome contém** para exibir os volumes cujos nomes contêm "abc".

b. Selecione **<<All Volumes whose name contains 'abc'>>** na área Recursos Disponíveis e mova-o para a área Recursos Selecionados.

c. Clique em **Excluir**, digite **`xyz`** no campo **O nome contém** e, em seguida, clique em **Adicionar**.

3. Clique em **Eventos** e selecione **Crítico** no campo Severidade do evento.
4. Selecione **Todos os eventos críticos** na área Eventos correspondentes e mova-o para a área Eventos selecionados.
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 durante um período específico. Você deve determinar o horário a partir do qual a notificação do 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 no Active IQ Unified Manager

Você pode adicionar alertas com base em um recurso, como um cluster, nó, agregado ou volume, e em eventos de um tipo de gravidade específico. Como prática recomendada, você pode adicionar um alerta para qualquer um dos seus objetos críticos depois de ter adicionado o cluster ao qual o objeto pertence.

Você pode usar as seguintes diretrizes e considerações para criar alertas para gerenciar seus sistemas com eficácia:

- Descrição do alerta

  Você deve fornecer uma descrição para o alerta para que isso ajude você a rastrear seus alertas com eficácia.

- Recursos

  Você deve decidir qual recurso físico ou lógico requer um alerta. Você pode incluir e excluir recursos, conforme necessário. Por exemplo, se você deseja monitorar de perto seus agregados configurando um alerta, você deve 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 dessa 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 em todos os clusters, receberá alertas apenas 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, deve decidir quais eventos exigem um alerta.

  Se você selecionar uma gravidade do evento, mas não selecionar nenhum evento individual (se deixar a coluna "Eventos Selecionados" vazia), você receberá alertas para todos os eventos da categoria.

- Ações

  Você deve fornecer os nomes de usuário e endereços de e-mail dos usuários que receberão a notificação. Você também pode especificar um trap 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 uma notificação repetidamente aos destinatários durante um período específico. Você deve determinar a partir de que horário a notificação do evento ficará ativa para o alerta. Se você quiser que a notificação do evento seja repetida até que o evento seja confirmado, deverá determinar com que frequência a notificação será repetida.

- Executar script

  Você pode associar seu script a um alerta. Seu script é executado quando o alerta é gerado.

Adicione alertas para eventos de desempenho no Active IQ Unified Manager

Você pode configurar alertas para eventos de desempenho individuais, assim como para qualquer outro evento recebido pelo Unified Manager. Além disso, se 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 ser notificado quando qualquer evento de desempenho crítico ou de aviso for acionado.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

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 à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
2. Na página **Alert Setup**, clique em **Add**.
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 está 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 de Gravidade do Evento, selecione **Crítico**.

b. No campo Nome do evento contém, digite **`latency`** e clique na seta para selecionar todos os eventos correspondentes.

c. No campo Nome do evento contém, digite **`iops`** e clique na seta para selecionar todos os eventos correspondentes.

d. No campo Nome do evento contém, digite **`mbps`** e clique na seta para selecionar todos os eventos correspondentes.

6. Clique em **Ações** e selecione o nome do usuário que receberá o e-mail de alerta no campo **Alertar estes usuários**.
7. Configure as outras opções nesta página para emitir traps SNMP e executar um script.
8. Clique em **Salvar**.

Teste alertas no Active IQ Unified Manager

Você pode testar um alerta para verificar se você o configurou corretamente. Quando um evento é acionado, um alerta é gerado, e um e-mail de alerta é enviado aos destinatários configurados. Você pode verificar se a notificação é enviada e se o seu script é 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 SNMP trap.

  O servidor do Unified Manager pode usar essas configurações para enviar notificações aos usuários quando um evento for gerado.

- Você deve ter atribuído um script e configurado o script para ser executado quando o alerta for gerado.
- Você precisa ter a função de Application Administrator.

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
2. Na página **Configuração de alertas**, 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.

Desative os alertas para eventos Resolvidos e Obsoletos no Active IQ Unified Manager

Para todos os eventos que você configurou para enviar alertas, uma mensagem de alerta é enviada quando esses eventos transitam por todos os estados disponíveis: Novo, Resolvido e Obsoleto. Se você não quiser receber alertas para eventos que passam para os estados Resolvido e Obsoleto, você pode configurar uma configuração global para suprimir esses alertas.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Por padrão, os alertas não são enviados para eventos quando eles passam para os estados Resolvido e Obsoleto.

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
2. Na página **Configuração de alertas**, 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 assim que os eventos forem resolvidos ou se tornarem obsoletos	Mova o controle deslizante para a direita

Exclua os volumes de destino de recuperação de desastres da geração de alertas no Active IQ Unified Manager

Ao configurar alertas de volume, você pode especificar uma string na caixa de diálogo Alerta que identifica um volume ou grupo de volumes. No entanto, se você configurou a recuperação de desastres para SVMs, os volumes de origem e de destino têm o mesmo nome, portanto, você receberá alertas para ambos os volumes.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Você pode desativar alertas para volumes de destino de recuperação de desastres excluindo volumes que tenham o nome da SVM de destino. Isso é possível porque o identificador de eventos de volume contém o nome da SVM e o nome do volume no formato "<svm_name>:/<volume_name>".

O exemplo abaixo mostra como criar alertas para o volume "vol1" na SVM primária "vs1", mas excluir a geração do alerta para um volume com o mesmo nome na SVM "vs1-dr".

Execute as etapas a seguir na caixa de diálogo Add Alert:

Passos

1. Clique em **Name** e insira um nome e uma descrição para o alerta.
2. Clique em **Recursos** e selecione a guia **Incluir**.
   a. Selecione **Volume** na lista suspensa e, em seguida, digite **`vol1`** no campo **Nome contém** para exibir os volumes cujo nome contém "vol1".
   b. Selecione **<<All Volumes whose name contains 'vol1'>>** na área **Recursos Disponíveis** e mova-o para a área **Recursos Selecionados**.
3. Selecione a guia **Excluir**, selecione **Volume**, digite **`vs1-dr`** no campo **O nome contém** e clique em **Adicionar**.

   Isso impede que o alerta seja gerado para o volume "vol1" na SVM "vs1-dr".
4. Clique em **Eventos** e selecione o(s) evento(s) que deseja aplicar ao(s) volume(s).

5. Clique em **Ações** e selecione o nome do usuário que receberá o e-mail de alerta no campo **Alertar estes usuários**.
6. Configure outras opções nesta página para emitir traps SNMP e executar um script e, em seguida, clique em **Salvar**.

Visualize os alertas no Active IQ Unified Manager

Na página Configuração de Alertas, você pode visualizar a lista de alertas criada para vários eventos. Você também pode visualizar as propriedades dos alertas, como a descrição do alerta, o método e a frequência de 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Etapa

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.

   A lista de alertas é exibida na página de Configuração de Alertas.

Editar alertas no Active IQ Unified Manager

Você pode editar as propriedades do 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 precisa ter a função de Application Administrator.

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
2. Na página **Configuração de alertas**, selecione o alerta que deseja editar e clique em **Editar**.
3. Na caixa de diálogo **Edit Alert**, 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 no Active IQ Unified Manager

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 precisa ter a função de Application Administrator.

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
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

Saiba mais sobre a página de Configuração de Alertas no Active IQ Unified Manager

A página de Configuração de Alertas exibe uma lista de alertas e fornece informações sobre o nome, o status, o método de notificação e a frequência de notificação de cada alerta. Você também pode adicionar, editar, remover, ativar ou desativar alertas nesta página.

Você precisa ter a função de Application Administrator ou Storage Administrator.

Botões de comando

- **Adicionar**

  Exibe a caixa de diálogo Add Alert, que permite adicionar novos alertas.

- **Editar**

  Exibe a caixa de diálogo Editar Alerta, que permite editar os alertas selecionados.

- **Excluir**

  Exclui os alertas selecionados.

- **Habilitar**

  Permite que os alertas selecionados enviem 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 ativar ou desativar o envio de alertas quando os eventos são movidos para os estados Resolved ou Obsolete. Isso pode ajudar os usuários a evitar o recebimento de notificações desnecessárias.

Visualização em lista

A visualização em 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 visualizar mais informações sobre ele na área de detalhes.

- **Status**

  Especifica se um alerta está ativado ( ) ou desativado ( ).

- **Alerta**

  Exibe o nome do alerta.

- **Descrição**

  Exibe uma descrição para o alerta.

- **Método de Notificação**

  Exibe o método de notificação selecionado para o alerta. Você pode notificar os usuários por e-mail ou por meio de 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 o qual você deseja acionar o alerta.

- **Exclui**

  Exibe o grupo de recursos para o qual 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.

Saiba mais sobre a caixa de diálogo Adicionar Alerta no Active IQ Unified Manager

Você pode criar alertas para ser notificado quando um evento específico for gerado, permitindo que você resolva o problema rapidamente e, assim, minimize o impacto em seu ambiente. Você pode criar alertas para um único recurso ou um conjunto de recursos, e para eventos de um determinado tipo de gravidade. Você também pode especificar o método de notificação e a frequência dos alertas.

Você precisa ter a função de Application Administrator ou Storage Administrator.

Nome

Esta área permite que você especifique um nome e uma descrição para o alerta:

- **Nome do alerta**

  Permite que você especifique um nome para o alerta.

- **Descrição do alerta**

  Permite especificar 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 quer acionar o alerta. Uma regra dinâmica é o conjunto de recursos filtrados com base na cadeia de texto que você especificar. 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 a partir de qualquer uma das páginas de detalhes do objeto de armazenamento, o objeto de armazenamento será incluído automaticamente no alerta.

- **Incluir**

  Permite incluir os recursos para os quais você deseja acionar alertas. Você pode especificar uma cadeia de texto para agrupar recursos que correspondam à cadeia e selecionar esse grupo para incluí-lo no

alerta. Por exemplo, você pode agrupar todos os volumes cujo nome contenha a cadeia "abc".

- **Excluir**

  Permite excluir recursos para os quais você não deseja acionar alertas. Por exemplo, você pode excluir todos os volumes cujo nome contenha a cadeia de texto "xyz".

  A guia Excluir é exibida somente quando você seleciona todos os recursos de um determinado tipo de recurso: por exemplo, <<All Volumes>> ou <<All Volumes whose name contains 'xyz'>>.

  Se um recurso estiver em conformidade com as regras de inclusão e exclusão que você especificou, a regra de exclusão terá precedência sobre a regra de inclusão, e o alerta não será gerado para o evento.

Eventos

Esta área permite selecionar os eventos para os quais você deseja criar alertas. Você pode criar alertas para eventos com base em uma determinada gravidade 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 Crítica, Erro ou Aviso.

- **O nome do evento contém**

  Permite selecionar eventos cujos nomes contenham os caracteres especificados.

Ações

Esta área permite que você especifique os usuários que deseja notificar quando um alerta for acionado. Você também pode especificar o método de notificação e a frequência das notificações.

- **Avise esses usuários**

  Permite que você especifique o endereço de e-mail ou o nome de usuário do usuário para receber notificações.

  Se você modificar o endereço de e-mail especificado para o usuário e reabrir o alerta para edição, o campo Name aparecerá em branco, pois o endereço de e-mail modificado não estará mais vinculado ao usuário que foi selecionado anteriormente. Além disso, se você tiver modificado o endereço de e-mail do usuário selecionado na página Users, 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 com a frequência especificada dentro do intervalo de tempo especificado

- **Emitir trap SNMP**

  Ao selecionar esta caixa, você pode especificar se os traps SNMP devem ser enviados para o host SNMP configurado globalmente.

- **Executar Script**

  Permite que você adicione seu script personalizado ao alerta. Esse script é executado quando um alerta é gerado.

> Se você não visualizar essa funcionalidade na interface de usuário, é porque seu administrador a desativou. Se necessário, você pode ativá-la 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.

Editar propriedades de alerta no Active IQ Unified Manager

Você pode editar as propriedades do alerta, como o recurso ao qual o alerta está associado, os eventos, o script e as opções de notificação.

Nome

Esta área permite editar o nome e a descrição do alerta.

- **Nome do alerta**

  Permite editar o nome do alerta.

- **Descrição do alerta**

  Permite especificar uma descrição para o alerta.

- **Estado de alerta**

  Permite que você ative ou desative o alerta.

Recursos

Esta área permite selecionar um recurso individual ou agrupar os recursos com base em uma regra dinâmica para a qual você deseja acionar o alerta. Você pode pesquisar recursos selecionando um tipo de recurso na lista suspensa ou especificar o nome exato do recurso para exibir um recurso específico.

- **Incluir**

  Permite incluir os recursos para os quais você deseja acionar alertas. Você pode especificar uma cadeia de texto para agrupar recursos que correspondam a ela e selecionar esse grupo para incluí-lo no alerta.

Por exemplo, você pode agrupar todos os volumes cujo nome contenha a sequência “vol0”.

- **Excluir**

  Permite excluir recursos para os quais você não deseja acionar alertas. Por exemplo, você pode excluir todos os volumes cujo nome contenha a string “xyz”.

  > A guia Exclude é exibida somente quando você seleciona todos os recursos de um determinado tipo de recurso, por exemplo, <<All Volumes>> ou <<All Volumes whose name contains 'xyz'>>.

Eventos

Esta área permite selecionar os eventos para os quais você deseja acionar os alertas. Você pode acionar um alerta para eventos com base em uma determinada gravidade ou para um conjunto de eventos.

- **Gravidade do evento**

  Permite selecionar eventos com base no tipo de gravidade, que pode ser Crítica, Erro ou Aviso.

- **O nome do evento contém**

  Permite selecionar eventos cujos nomes contenham os caracteres especificados.

Ações

Esta área permite que você especifique o método de notificação e a frequência da notificação.

- **Avise esses usuários**

  Permite editar o endereço de e-mail ou o nome de usuário, ou especificar um novo endereço de e-mail ou nome de usuário para receber notificações.

- **Frequência de notificação**

  Permite editar a frequência com que o servidor de gerenciamento envia notificações até que o evento seja reconhecido, resolvido ou movido para o estado obsoleto.

  Você pode escolher os seguintes métodos de notificação:

  - Notificar apenas uma vez
  - Notificar com uma frequência específica
  - Notificar com a frequência especificada dentro do intervalo de tempo especificado

- **Emitir trap SNMP**

  Permite que você especifique se as traps SNMP devem ser enviadas ao host SNMP configurado globalmente.

- **Executar Script**

  Permite que você associe um script ao alerta. Esse 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

Gerencie scripts no Active IQ Unified Manager

Você pode usar scripts para modificar ou atualizar automaticamente vários objetos de armazenamento no Unified Manager. O script está associado a um alerta. Quando um evento aciona um alerta, o script é executado. Você pode carregar scripts personalizados e testar sua execução quando um alerta é gerado.

A capacidade de carregar scripts no Unified Manager e executá-los está habilitada por padrão. Se sua organização não quiser permitir essa funcionalidade por motivos de segurança, você pode desativá-la em **Storage Management** > **Feature Settings**.

Informações relacionadas

"Habilitar e desabilitar a capacidade de carregar scripts"

Como os scripts funcionam com alertas no Active IQ Unified Manager

Você pode associar um alerta ao seu script para que ele seja executado quando um alerta for acionado para um evento no Unified Manager. Você pode usar os scripts para resolver problemas com objetos de armazenamento ou identificar quais objetos de armazenamento estão gerando os eventos.

Quando um alerta é gerado para um evento no Unified Manager, um e-mail de alerta é enviado aos destinatários especificados. Se você associou um alerta a um script, o script é executado. Você pode obter os detalhes dos argumentos passados para o 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 "Fix it" não estarão disponíveis por padrão na página Management Actions nem no dashboard do Unified Manager.

O script utiliza os seguintes argumentos para execução:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`

- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Você pode usar os argumentos em seus scripts e coletar informações sobre eventos relacionados ou modificar objetos de armazenamento.

Exemplo de obtenção de argumentos a partir 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 no Active IQ Unified Manager

Você pode adicionar scripts no Unified Manager e associar os scripts a alertas. Esses scripts são executados automaticamente quando um alerta é gerado e permitem que você obtenha informações sobre os 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 compatíveis 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 em Perl, Python e Shell
Windows	PowerShell, scripts Perl, Python e .bat

  - Para scripts em Perl, o Perl deve estar instalado no servidor do Unified Manager. Para instalações do VMware, o Perl 5 é instalado por padrão, e os scripts oferecerão suporte apenas ao que o Perl 5 suporta. Se o Perl foi instalado após o Unified Manager, você deve reiniciar o servidor do Unified Manager.
  - Para scripts PowerShell, a política de execução apropriada do PowerShell deve ser configurada no servidor Windows para que os scripts possam ser executados.

> Se o seu script criar arquivos de log para acompanhar o progresso do script de alerta, você deve garantir que esses arquivos de log não sejam criados em nenhum lugar dentro da

pasta de instalação do Unified Manager.

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Você pode fazer upload de scripts personalizados e coletar detalhes do evento sobre o alerta.

Se você não visualizar essa funcionalidade na interface de usuário, é porque seu administrador a desativou. Se necessário, você pode ativá-la 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 **Add**.

Informações relacionadas

"Habilitar e desabilitar a capacidade de carregar scripts"

Excluir scripts no Active IQ Unified Manager

Você pode excluir um script do Unified Manager quando ele não for mais necessário ou válido.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- O script não deve estar associado a um alerta.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Scripts**.
2. Na página **Scripts**, selecione o script que deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

Execução de script de teste no Active IQ Unified Manager

Você pode verificar se seu script é executado corretamente quando um alerta é gerado para um objeto de armazenamento.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você deve ter carregado no Unified Manager um script em um formato de arquivo compatível.

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 à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
4. Na página **Configuração de alertas**, execute uma das seguintes ações:

Para…	Faça isso…
Adicionar um alerta	a. Clique em **Add**. 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 **Alert Setup**, selecione o alerta que você adicionou ou modificou e clique em **Test**.

   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.

Saiba mais sobre os comandos da CLI do Active IQ Unified Manager compatíveis

Como administrador de storage, você pode usar os comandos da CLI para executar consultas em objetos de storage; por exemplo, em clusters, agregados, volumes, qtrees e LUNs. Você pode usar os comandos da CLI para consultar o banco de dados interno do Unified Manager e o banco de dados do ONTAP. Você também pode usar comandos da CLI em scripts que são executados no início ou no final de uma operação ou quando um alerta é acionado.

Todos os comandos devem ser precedidos pelo comando `um cli login` e por 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
`um cli login -u <username> [-p <password>]`	Faz login na CLI. Devido a questões de segurança, você deve inserir apenas o nome de usuário após a opção "-u". Quando usado dessa forma, o sistema solicitará sua senha, e a senha não será registrada no histórico nem na tabela de processos. A sessão expira três horas após o login, depois disso, você deve fazer login novamente.	Exibe a mensagem correspondente.
`um cli logout`	Encerra a sessão na CLI.	Exibe a mensagem correspondente.

Comando CLI	Descrição	Saída
`um help`	Exibe todos os subcomandos de primeiro nível.	Exibe todos os subcomandos de primeiro nível.
`um run cmd [ -t <timeout> ] <cluster> <command>`	A maneira mais simples de executar um comando em um ou mais hosts. Usado principalmente para scripts de alerta para obter ou executar uma operação no ONTAP. O argumento opcional timeout define um limite máximo de tempo (em segundos) para o comando ser concluído no cliente. O padrão é 0 (esperar indefinidamente).	Conforme recebido do ONTAP.
`um run query <sql command>`	Executa uma consulta SQL. Somente consultas que leem do banco de dados são permitidas. Operações de atualização, inserção ou exclusão não são suportadas.	Os resultados são exibidos em formato de tabela. Se um conjunto vazio for retornado ou se houver algum erro de sintaxe ou solicitação inválida, o sistema exibe a mensagem de erro apropriada.
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Adiciona uma fonte de dados à lista de sistemas de storage gerenciados. Uma fonte de dados descreve como as conexões com os sistemas de storage são feitas. As opções -u (nome de usuário) e -P (senha) devem ser especificadas ao adicionar uma fonte de dados. A opção -t (protocolo) especifica o protocolo usado para se comunicar com o cluster (http ou https). Se o protocolo não for especificado, ambos os protocolos serão tentados A opção -p (porta) especifica a porta usada para se comunicar com o cluster. Se a porta não for especificada, o valor padrão do protocolo apropriado será tentado. Este comando só pode ser executado pelo administrador de storage.	Solicita que você 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.`

Comando CLI	Descrição	Saída
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	Modifica uma ou mais opções da fonte de dados. Só pode ser executado pelo administrador de storage.	Exibe a mensagem correspondente.
`um datasource remove <datasource-id>`	Remove a fonte de dados (cluster) do Unified Manager.	Exibe a mensagem correspondente.
`um option list [ <option> .. ]`	Lista todas as opções que você pode configurar usando o comando set.	Exibe os seguintes valores em formato tabular: `Name, Value, Default Value, and Requires Restart.`
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	Define uma ou mais opções. O comando só pode ser executado pelo administrador de storage.	Exibe a mensagem correspondente.
`um version`	Exibe a versão do software do Unified Manager.	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	Lista os LUNs após filtrar pelo objeto especificado. O parâmetro -q é aplicável a todos os comandos para não exibir cabeçalho. ObjectType pode ser lun, qtree, cluster, volume, quota ou svm. Por exemplo: **`um lun list -cluster 1`** 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.`
`um svm list [-q] [ -ObjectType <object-id>]`	Lista as VMs de armazenamento após filtrar pelo objeto especificado. ObjectType pode ser lun, qtree, cluster, volume, quota ou svm. Por exemplo: **`um svm list -cluster 1`** Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todas as VMs de storage no 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 os qtrees após filtrar pelo objeto especificado. O parâmetro -q é aplicável a todos os comandos para não exibir 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 todos os qtrees no 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 no 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 disk, aggr, node, 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
`um cluster node list [-q] [-ObjectType <object-id>]`	Lista os nós do cluster após filtrar pelo objeto especificado. ObjectType pode ser disk, aggr, node ou cluster. Por exemplo: **`um cluster node list -cluster 1`** Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os nós no cluster com ID 1.	Exibe os seguintes valores em formato tabular `Name and Cluster ID`.
`um volume list [-q] [-ObjectType <object-id>]`	Lista os volumes após filtrar pelo objeto especificado. ObjectType pode ser lun, qtree, cluster, volume, quota, svm ou aggregate. Por exemplo: **`um volume list -cluster 1`** Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os volumes no cluster com ID 1.	Exibe os seguintes valores em formato tabular `Volume ID and Volume Name`.
`um quota user list [-q] [-ObjectType <object-id>]`	Lista os usuários de cota após filtrar pelo objeto especificado. ObjectType pode ser qtree, cluster, volume, quota ou svm. Por exemplo: **`um quota user list -cluster 1`** Neste exemplo, "-cluster" é o objectType e "1" é o objectId. O comando lista todos os usuários de cota no cluster com ID 1.	Exibe os seguintes valores em formato tabular `ID, Name, SID and Email`.

Comando CLI	Descrição	Saída
`um aggr list [-q] [-ObjectType <object-id>]`	Lista os agregados após filtrar pelo objeto especificado. ObjectType pode ser disco, agregado, 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 no cluster com ID 1.	Exibe os seguintes valores em formato tabular `Aggr ID, and Aggr Name`.
`um event ack <event-ids>`	Reconhece um ou mais eventos.	Exibe a mensagem correspondente.
`um event resolve <event-ids>`	Resolve um ou mais eventos.	Exibe a mensagem correspondente.
`um event assign -u <username> <event-id>`	Atribui um evento a um usuário.	Exibe a mensagem correspondente.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Lista os eventos gerados pelo sistema ou pelo usuário. Filtra os eventos com base na origem, no estado e nos IDs.	Exibe os seguintes valores em formato tabular `Source, Source type, Name, Severity, State, User and Timestamp`.
`um backup restore -f <backup_file_path_and_name>`	Restaura um backup de banco de dados MySQL usando arquivos .7z.	Exibe a mensagem correspondente.

Descrição das janelas de script e caixas de diálogo

Saiba mais sobre a página de Scripts no Active IQ Unified Manager

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 em lista

A visualização em 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 no Active IQ Unified Manager

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 precisa ter a função de Application Administrator ou Storage Administrator.

- **Selecione o arquivo de script**

  Permite selecionar 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

Saiba mais sobre monitoramento de desempenho no Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente OnCommand Unified Manager) oferece recursos de monitoramento de desempenho e análise da causa raiz de eventos para sistemas que executam o software NetApp ONTAP.

O Unified Manager ajuda você a identificar cargas de trabalho que estão sobrecarregando 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 ultrapassado. 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 volumes FlexGroup que você criou em seu cluster.

- Cargas de trabalho definidas pelo sistema

  Essas cargas de trabalho consistem em atividades internas do sistema.

Explore os recursos de monitoramento de desempenho do Active IQ 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 diversos componentes do cluster.

Um alto tempo de resposta (latência) indica que o objeto de armazenamento, por exemplo, um volume, está apresentando desempenho inferior ao normal. Esse problema também indica que houve queda no desempenho dos aplicativos cliente que usam 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 realizar para resolver o problema de desempenho.

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.
- Monitora contadores de desempenho para clusters, nós, agregados, portas, SVMs, volumes, LUNs, namespaces NVMe e interfaces de rede (LIFs).

- Exibe gráficos detalhados que representam 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 proporção de cache.
- Permite criar políticas de limite de desempenho definidas pelo usuário que disparam eventos e enviam alertas por e-mail quando os limites são ultrapassados.
- Utiliza limites definidos pelo sistema e limites de desempenho dinâmicos que aprendem sobre a atividade da sua carga de trabalho para identificar e alertar você sobre problemas de desempenho.
- Identifica as políticas de qualidade do serviço (QoS) e as políticas de Nível de Serviço de Desempenho (PSLs) aplicadas aos seus volumes e LUNs.
- Identifica claramente o componente do cluster que está em disputa.
- Identifica cargas de trabalho que estão sobrecarregando os componentes do cluster e as cargas de trabalho cujo desempenho é afetado pelo aumento da atividade.

Use as interfaces do Active IQ Unified Manager para gerenciar o desempenho do sistema de storage

Estas seções contêm informações sobre as duas interfaces de usuário que o Active IQ Unified Manager oferece para solucionar problemas de capacidade, disponibilidade e proteção no storage de dados. As duas interfaces de usuário são a interface da Web do Unified Manager e o console de manutenção.

Se você deseja usar os recursos de proteção do Unified Manager, também precisa 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 do cluster relacionados à capacidade de storage, disponibilidade e proteção de dados.

Estas seções descrevem alguns fluxos de trabalho comuns que um administrador pode seguir para solucionar problemas de capacidade de storage, disponibilidade de dados ou proteção exibidos na interface 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 de usuários e problemas de rede relacionados ao próprio servidor do Unified Manager. Se a interface web do Unified Manager estiver indisponível, 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 utilizá-las para resolver problemas relacionados ao funcionamento do servidor Unified Manager.

Visualize a configuração do cluster e os dados de desempenho no Active IQ Unified Manager

O intervalo de coleta de *dados de configuração do cluster* é de 15 minutos. Por exemplo, depois que você adiciona um cluster, leva 15 minutos para exibir os detalhes do cluster na UI do Unified Manager. Esse intervalo também se aplica quando você faz 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 polling, que pode ser de até 15 minutos.

O Unified Manager coleta estatísticas de desempenho atuais de todos os clusters monitorados a cada cinco minutos. Ele analisa esses dados para identificar eventos de desempenho e possíveis problemas. O sistema retém 30 dias de dados históricos de desempenho a cada cinco minutos e 180 dias de dados históricos de desempenho a cada hora. Isso permite que você visualize detalhes de desempenho muito granulares para o mês atual e tendências gerais de desempenho por até um ano.

As sondagens de coleta são defasadas em alguns minutos para que os dados de todos os clusters não sejam enviados ao mesmo tempo, o que poderia 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, pelo sistema e dinâmicos. Caso algum limite de desempenho seja ultrapassado, o Unified Manager gera eventos e envia e-mails para os usuários especificados, se configurado para isso.
Sondagem 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 12 coletas de dados de desempenho mais recentes de cinco minutos em médias horárias. Os valores médios por hora são usados em algumas páginas da UI e são mantidos por 180 dias.
Análise de previsão e eliminação de dados	Todos os dias depois da meia-noite	Analisa dados do cluster para estabelecer limites dinâmicos de latência 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
Eliminação de dados	Todos os dias depois das 02:00.	Exclui do banco de dados quaisquer eventos com mais de 180 dias e limiares dinâmicos com mais de 180 dias.
Eliminação de dados	Todos os dias depois das 3h30 da manhã	Exclui do banco de dados quaisquer dados de desempenho de uma hora com mais de 180 dias.

Compreenda os ciclos de coleta de continuidade de dados no Active IQ Unified Manager

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 nos dados estatísticos que ocorrem quando não foi possível coletar dados em tempo real.

O Unified Manager realiza pesquisas de coleta de continuidade de dados dos dados históricos de desempenho quando os seguintes eventos ocorrem:

- Inicialmente, um cluster é adicionado ao Unified Manager.

  O Unified Manager coleta dados históricos de desempenho dos últimos 15 dias. Isso permite que você visualize duas semanas de informações históricas de desempenho de um cluster poucas horas após sua adição.

  Além disso, o sistema relata os eventos de limite do período anterior, se houver.

- 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 será ignorado.

- O Unified Manager ficou inacessível por um período de tempo e depois voltou 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 corrigida.
- Um cluster ficou inacessível por um período de tempo e depois voltou a ficar online, como nas seguintes situações:
  - Uma interrupção de rede é corrigida.
  - Uma conexão de rede de longa distância lenta atrasou a coleta normal de dados de desempenho.

Um ciclo de coleta de continuidade de dados pode coletar no máximo 24 horas de dados históricos. Se o Unified Manager ficar inativo por mais de 24 horas, uma lacuna nos dados de desempenho aparecerá nas páginas da interface de 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 ser concluído antes que a coleta de dados de desempenho em tempo real seja iniciada. Quando a coleta de continuidade de dados precisa coletar mais de uma hora de dados históricos, você vê uma mensagem de banner para esse cluster na parte superior do painel Notifications.

Saiba mais sobre os registros de data e hora nos dados e eventos coletados no Active IQ Unified Manager

O registro de data e hora que aparece nos dados de saúde e desempenho coletados, ou que aparece como o horário de detecção de um evento, é baseado na hora do cluster ONTAP, ajustada ao fuso horário definido no navegador da web.

É altamente recomendável que você use um servidor NTP (Network Time Protocol) para sincronizar a hora nos seus servidores do Unified Manager, nos clusters do ONTAP e nos navegadores da web.

Se você vir carimbos de data e hora que parecem incorretos para um determinado cluster, talvez seja necessário verificar se o horário do cluster está configurado corretamente.

Navegando pelos fluxos de trabalho de desempenho na interface gráfica do Unified Manager

Navegue pelos fluxos de trabalho de desempenho na interface gráfica do Active IQ Unified Manager

A interface do Unified Manager oferece muitas páginas para a coleta e a exibição de informações de desempenho. Você usa o painel de navegação à esquerda para navegar até as páginas na GUI e usa guias e links nas páginas para visualizar e configurar informações.

Você utiliza todas as páginas a seguir para monitorar e solucionar problemas relacionados ao desempenho do cluster:

- página do dashboard
- 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

Faça login na interface do usuário do Active IQ Unified Manager

Você pode fazer login na interface de usuário do Unified Manager usando um navegador da web compatível.

Antes de começar

- O navegador web deve atender aos requisitos mínimos.

  Consulte a Interoperability Matrix em "mysupport.netapp.com/matrix" para obter a lista completa das

versões de navegador compatíveis.

- Você precisa ter o endereço IP ou a URL do servidor do Unified Manager.

A sessão é encerrada automaticamente após 1 hora de inatividade. Esse período pode ser configurado em **Geral** > **Configurações de recursos**.

Passos

1. Digite a URL no seu navegador da web, em que URL é o endereço IP ou o 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 aceitar o risco para continuar o acesso ou instalar um certificado digital assinado por uma Autoridade Certificadora (CA) para autenticação do servidor. . Na tela de login, insira 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 Dashboard é exibida.

> Se o servidor do Unified Manager não estiver inicializado, uma nova janela do navegador exibirá o assistente de primeira experiência. Você deve inserir um destinatário de e-mail inicial para o qual os alertas por e-mail serão enviados, o servidor SMTP que tratará as comunicações por e-mail e se o AutoSupport está habilitado para enviar informações sobre a instalação do Unified Manager para o suporte técnico. A interface de usuário do Unified Manager aparece depois que você conclui essas informações.

Interface gráfica e caminhos de navegação

Explore a interface gráfica e os caminhos de navegação no Active IQ Unified Manager

O Unified Manager oferece grande flexibilidade e permite que você realize diversas tarefas de várias maneiras. Há muitos caminhos de navegação que você descobrirá ao trabalhar no Unified Manager. Embora nem todas as combinações possíveis de navegação possam ser mostradas, você deve se familiarizar com alguns dos cenários mais comuns.

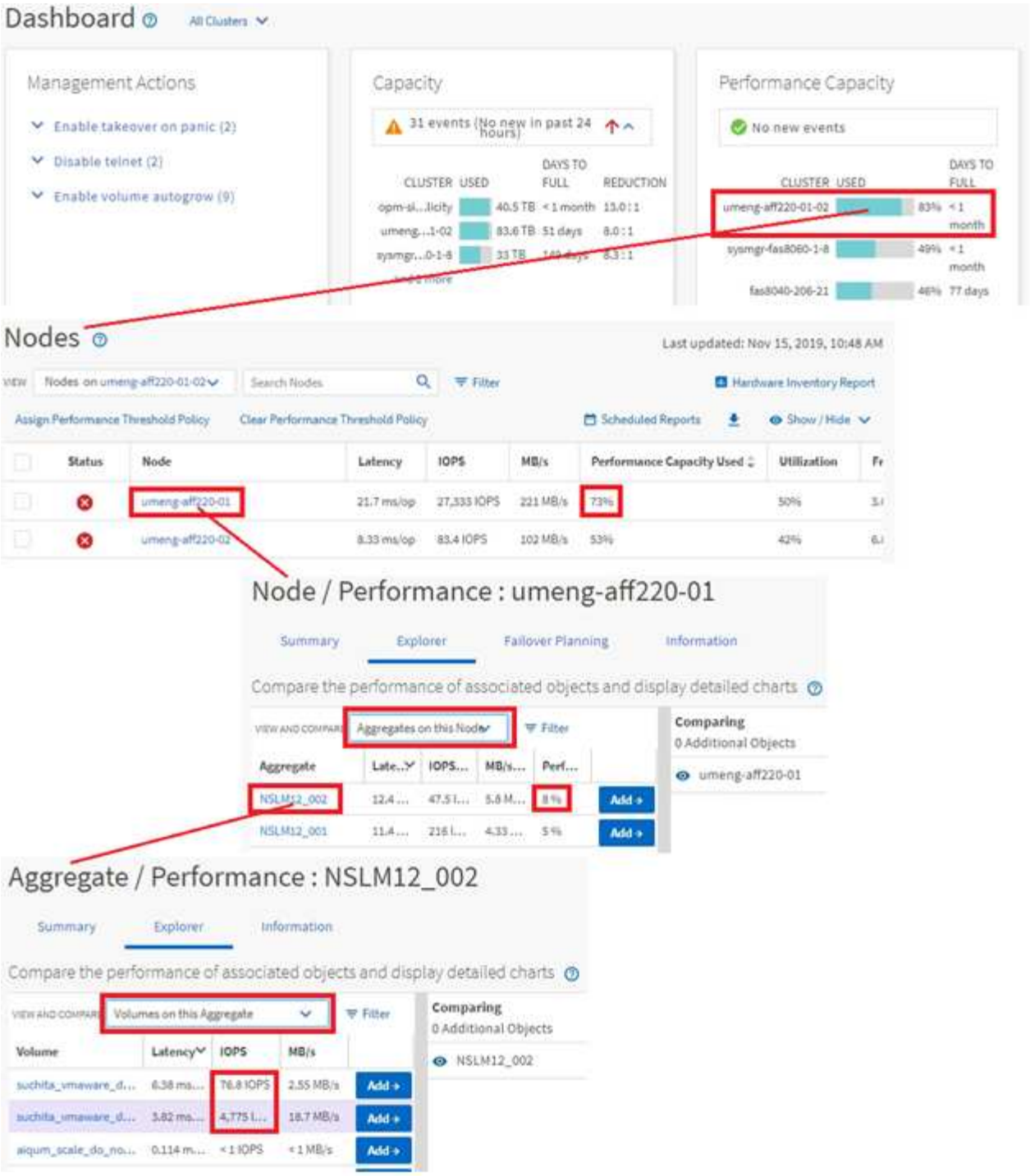
Monitore a navegação de objetos do cluster no Active IQ Unified Manager

Você pode monitorar o desempenho de todos os objetos em qualquer cluster gerenciado pelo Unified Manager. Monitorar seus objetos de armazenamento fornece uma visão geral do desempenho do cluster e dos objetos, e inclui o monitoramento de eventos de desempenho. Você pode visualizar o desempenho e os eventos em um alto nível ou investigar mais detalhadamente qualquer detalhe do desempenho dos objetos e dos eventos de desempenho.

Este é um exemplo de uma das muitas navegações possíveis entre objetos do cluster:

1. Na página do Painel de Controle, revise os detalhes no painel Capacidade de Desempenho para identificar o cluster que está utilizando a maior parte da 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 utilizada e clique nesse nó.
3. Na página Nó / Explorador de desempenho, clique em **Agregados neste nó** no menu Exibir e comparar.
4. Identifique o agregado que está utilizando a maior parte da capacidade de desempenho e clique nesse agregado.
5. Na página Aggregate / Performance Explorer, clique em **Volumes on this Aggregate** no menu View and Compare.
6. Identifique os volumes que estão usando mais IOPS.

Você deve investigar esses volumes para verificar 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 utilizem uma porcentagem tão grande de IOPS no cluster.



Monitore a navegação de desempenho do cluster no Active IQ Unified Manager

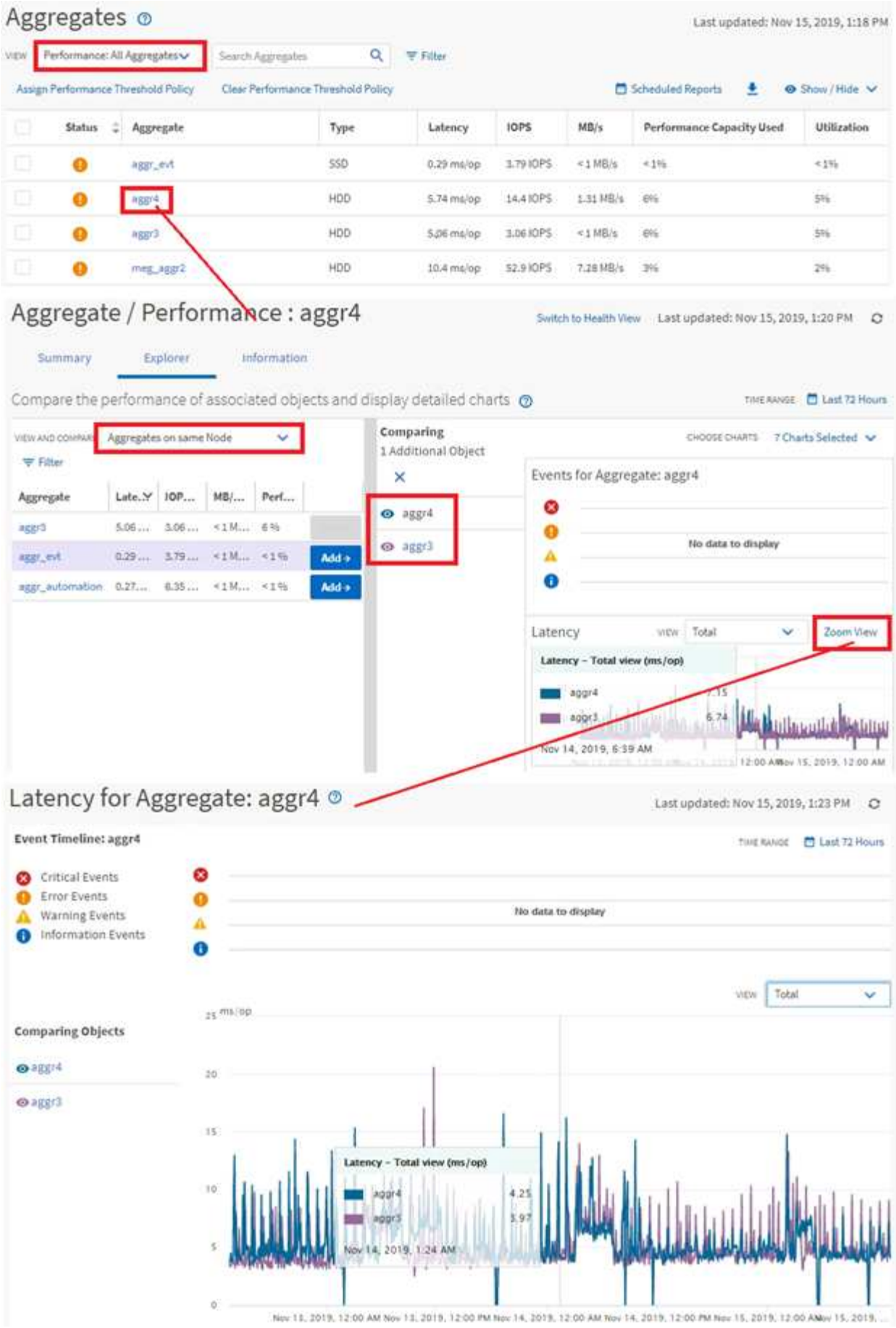
Você pode monitorar o desempenho de todos os clusters gerenciados pelo Unified Manager. O monitoramento de seus clusters fornece uma visão geral do desempenho do cluster e dos objetos e inclui o monitoramento de eventos de desempenho. Você pode visualizar o desempenho e os eventos em alto nível ou investigar mais detalhadamente qualquer detalhe do desempenho do cluster e dos objetos e dos eventos de desempenho.

Este é um exemplo de muitos caminhos de navegação possíveis para o desempenho de um cluster:

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Agregados**.
2. Para visualizar informações sobre o desempenho nesses agregados, selecione a visualização Desempenho: todos os agregados.
3. Identifique o agregado que você deseja investigar e clique no nome desse agregado para navegar até a página Aggregate / Performance Explorer.
4. Opcionalmente, selecione outros objetos para comparar com este agregado no menu Exibir e Comparar e, em seguida, adicione um dos objetos ao painel de comparação.

   As estatísticas de ambos os objetos aparecerão nos gráficos do contador para comparação.

5. No painel Comparing, à direita na página Explorer, clique em **Zoom View** em um dos gráficos de contador para ver 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%
aggr4
HDD
5.74 ms/op
14.4 IOPS
1.31 MB/s
6%
5%
aggr3
HDD
5.06 ms/op
3.06 IOPS
< 1 MB/s
6%
5%
meg_aggr2
HDD
10.4 ms/op
52.9 IOPS
7.28 MB/s
3%
2%
Aggregate / Performance : aggr4
Switch to Health View
Last updated: Nov 15, 2019, 1:20 PM
Summary
Explorer
Information
Compare the performance of associated objects and display detailed charts
TIME RANGE
Last 72 Hours
VIEW AND COMPARE
Aggregates on same Node
Filter
Aggregate
Late...
IOP...
MB/...
Perf...
aggr3
5.06 ...
3.06 ...
< 1 M...
6 %
aggr_evt
0.29 ...
3.79 ...
< 1 M...
< 1 %
Add
aggr_automation
0.27...
6.35 ...
< 1 M...
< 1 %
Add
Comparing
1 Additional Object
CHOOSE CHARTS
7 Charts Selected
aggr4
aggr3
Events for Aggregate: aggr4
No data to display
Latency
VIEW
Total
Zoom View
Latency – Total view (ms/op)
aggr4
7.15
aggr3
6.74
Nov 14, 2019, 6:39 AM
12:00 AM
Nov 15, 2019, 12:00 AM
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
VIEW
Total
Comparing Objects
aggr4
aggr3
ms/op
25
20
15
10
5
0
Latency – Total view (ms/op)
aggr4
4.25
aggr3
3.97
Nov 14, 2019, 1:24 AM
Nov 13, 2019, 12:00 AM
Nov 13, 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,

Investigar eventos de desempenho no Active IQ Unified Manager

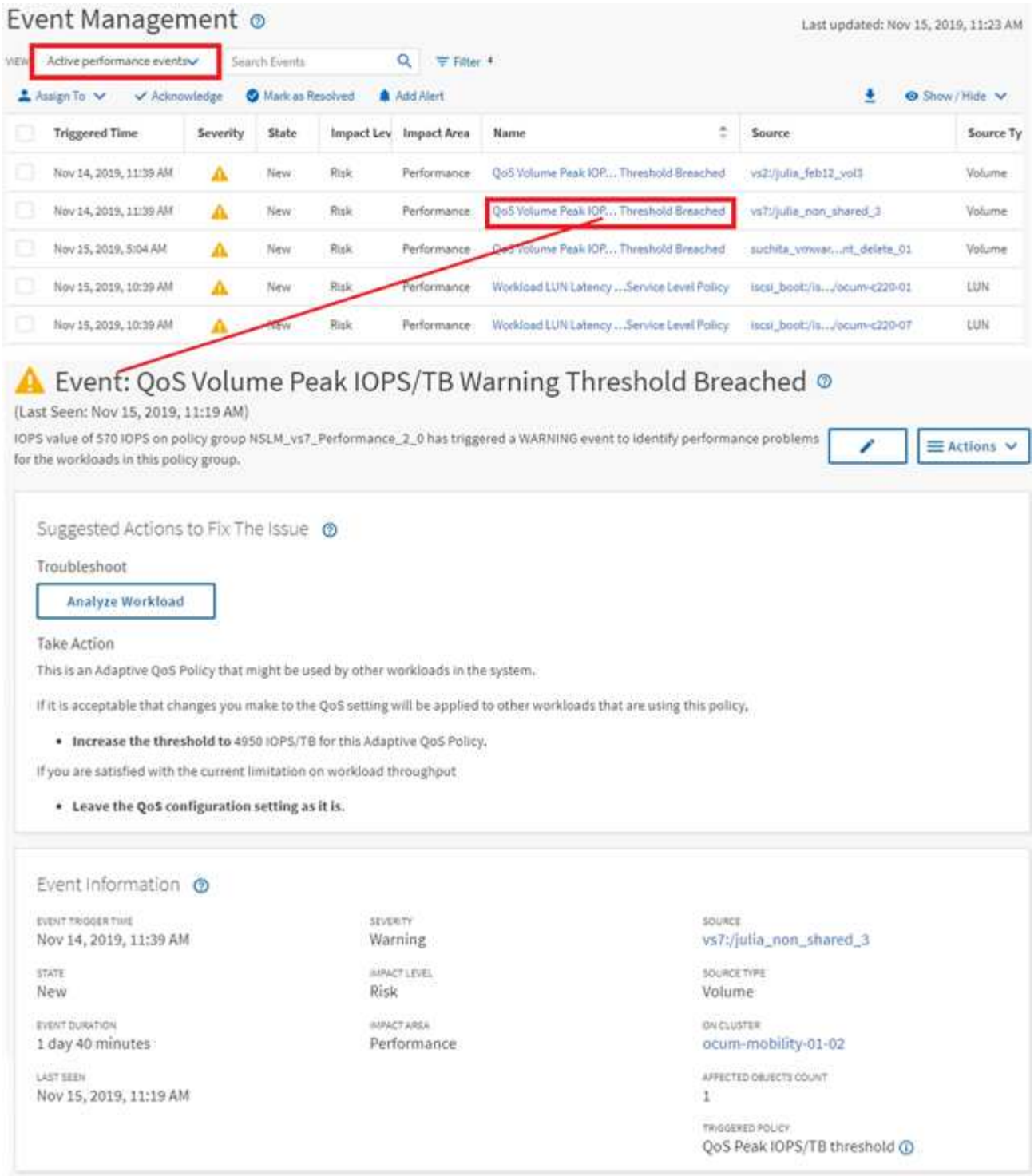
As páginas de detalhes de eventos do Unified Manager fornecem a você uma visão aprofundada de qualquer evento de desempenho. Isso é útil ao investigar eventos de desempenho, solucionar problemas e ajustar o desempenho do sistema.

Dependendo do tipo de evento de desempenho, 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 para investigação de eventos.

1. No painel de navegação à esquerda, clique em **Event Management**.
2. No menu Exibir, clique em **Eventos de desempenho ativos**.
3. Clique no nome do evento que você deseja investigar, e a página de detalhes do evento será exibida.
4. Veja a descrição do evento e 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 que ajudam a analisar melhor o problema.



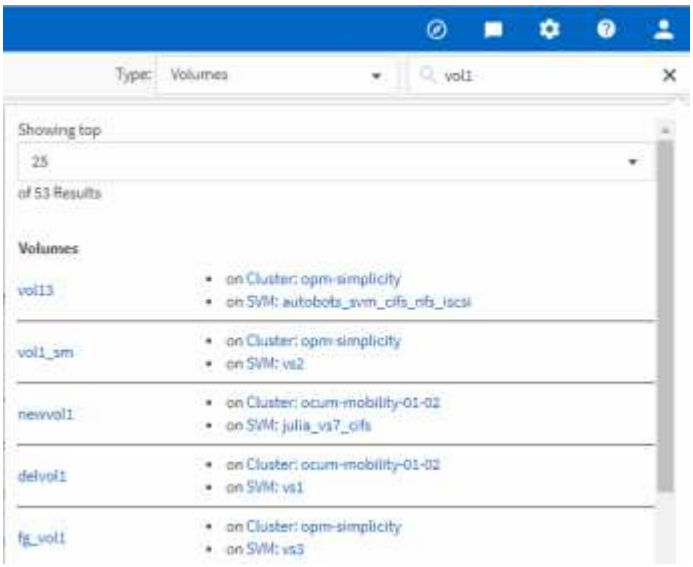
Pesquise objetos de armazenamento no Active IQ Unified Manager

Para acessar rapidamente um objeto específico, você pode usar o campo **Pesquisar todos os objetos de armazenamento** na parte superior da barra de menu. Esse método de pesquisa global em todos os objetos permite localizar rapidamente objetos específicos por tipo. Os resultados da pesquisa são classificados por tipo de objeto de armazenamento e você pode filtrá-los usando o menu suspenso. Uma pesquisa válida deve conter pelo menos três caracteres.

A busca global exibe o número total de resultados, mas apenas os 25 primeiros resultados de busca são acessíveis. Por isso, a funcionalidade de busca global pode ser considerada uma ferramenta de atalho para encontrar itens específicos, caso você já saiba quais itens deseja localizar rapidamente. Para obter resultados de busca completos, você pode usar a busca nas páginas de inventário de objetos e suas respectivas funcionalidades de filtro.

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 SVMs
- Volumes: nomes dos volumes
- LUNs: caminhos LUN



Não é possível pesquisar LIFs e portas na barra de pesquisa global.

Neste exemplo, a caixa suspensa tem o tipo de objeto Volume selecionado. Digitar “vol” no campo **Search all Storage Objects** 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 Performance Explorer desse objeto. Para pesquisas de eventos, clicar em um item no resultado da pesquisa leva você até a página Event Details.

Filtre o conteúdo da página de inventário no Active IQ Unified Manager

Você pode filtrar os dados da página de inventário do Unified Manager para localizar rapidamente os dados com base em critérios específicos. Você pode usar a filtragem para restringir o conteúdo das páginas do Unified Manager e mostrar apenas os resultados nos quais você tem interesse. Isso proporciona um método muito eficiente de exibir apenas os dados nos quais você tem interesse.

Use a opção **Filtragem** para personalizar a visualização em grade de acordo com suas preferências. As opções de filtro disponíveis se baseiam no tipo de objeto visualizado na grade. Se houver filtros aplicados no momento, o número de filtros aplicados será exibido à direita do botão Filter.

Há suporte para três tipos de parâmetros de filtro.

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**.

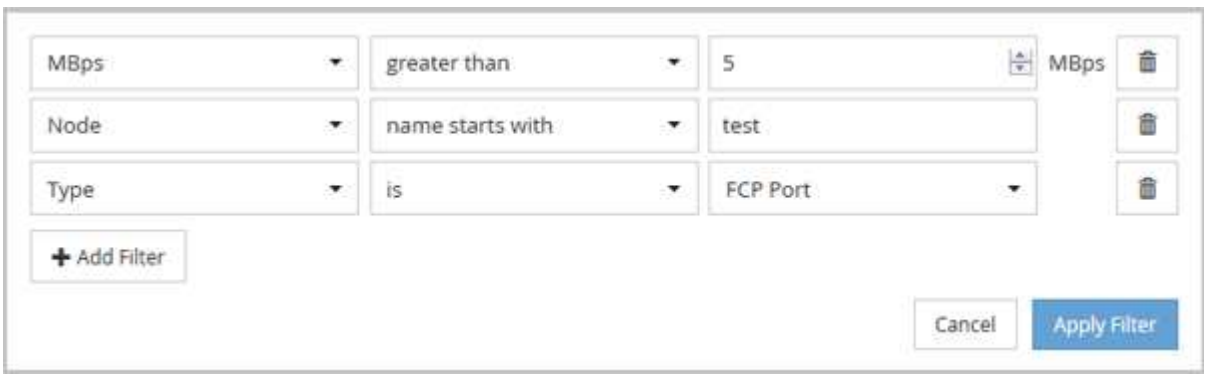
Os campos Coluna, Operador e Valor são obrigatórios para cada filtro; os filtros disponíveis refletem as colunas filtráveis na página atual. O número máximo de filtros que você pode aplicar é quatro. Os resultados filtrados são baseados na combinação dos parâmetros de filtro. Os resultados filtrados se aplicam a todas as páginas da sua pesquisa filtrada, não apenas à página exibida no momento.

Você pode adicionar filtros usando o painel de Filtragem.

1. Na parte superior da página, clique no botão **Filtrar**. O painel de 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 desse objeto.
5. Para adicionar outro filtro, clique em **+Add Filter**. Um campo de filtro adicional é exibido. Preencha este filtro usando o processo descrito nas etapas anteriores. Observe que, ao adicionar o seu quarto filtro, o botão **+Add Filter** não é 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 de filtragem para remover filtros individuais clicando no ícone da lixeira à direita do filtro que você deseja remover.
8. Para remover todos os filtros, clique em **Reset** na parte inferior do painel de filtragem.

Exemplo de filtragem

A ilustração mostra o painel de filtragem com três filtros. O botão **+Adicionar Filtro** é exibido quando você tem menos de quatro filtros, o limite máximo.



Após clicar em **Aplicar filtro**, o painel de filtragem fecha, aplica seus filtros e mostra o número de filtros aplicados ().

Monitore o desempenho do cluster no Dashboard

Monitore o desempenho do cluster a partir do painel no Active IQ Unified Manager

O Dashboard 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 registre, localize ou atribua rapidamente para resolução quaisquer eventos específicos identificados.

Analise os painéis de desempenho no Active IQ Unified Manager Dashboard

O painel do Unified Manager fornece alguns painéis que exibem o status de desempenho de alto nível de todos os clusters que estão sendo monitorados no seu ambiente. Você pode optar por visualizar o status de todos os clusters ou de um cluster individual.

Além de exibir informações de desempenho, a maioria dos painéis também mostra 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 podem precisar de análise mais detalhada 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 dessa 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 para cada cluster (média da última 1 hora) e o número de dias até que a capacidade de desempenho atinja o limite superior (com base na taxa de crescimento diário). Clicar no gráfico de barras leva você à página de inventário de nós desse 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 total de IOPS e os valores totais de taxa de transferência.

- **Painel de IOPS da carga de trabalho**

  Quando o gerenciamento ativo de cargas de trabalho está habilitado e, ao visualizar um único cluster, este painel exibe o número total de cargas de trabalho que estão em execução no momento em uma determinada faixa de IOPS.

- **Painel de desempenho da carga de trabalho**

  Quando o gerenciamento ativo de cargas de trabalho está habilitado, este painel exibe o número total de cargas de trabalho em conformidade e não conformes 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 Workloads.

- **Painel de visão geral do uso**

  Ao visualizar todos os clusters, você pode optar por exibi-los classificados pelo maior IOPS ou pela taxa de transferência (MB/s).

  Ao visualizar um único cluster, você pode optar por visualizar as cargas de trabalho nesse cluster classificadas pelo maior número de IOPS ou pela maior taxa de transferência (MB/s).

Interpretar mensagens de banners de desempenho no Active IQ Unified Manager

O Unified Manager pode exibir mensagens de banner na página Notificações (acessível pelo sino de notificações) para alertar você sobre problemas de status em um cluster específico.

Mensagem do banner	Descrição	Resolução
`No performance data is being collected from cluster cluster_name. 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 cluster_name. Current data collections will start after all historical data is collected.`	Atualmente, está em execução um ciclo de coleta de continuidade de dados 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.

Altere o intervalo de coleta de estatísticas de desempenho no Active IQ Unified Manager

O intervalo de coleta padrão para estatísticas é de 5 minutos. Você pode alterar esse intervalo para 10 ou 15 minutos se perceber que as coletas de clusters grandes não estão sendo concluídas dentro do tempo padrão. Essa configuração afeta a coleta de estatísticas de todos os clusters que esta instância do Unified Manager está monitorando.

Antes de começar

Você precisa ter um ID de usuário e uma senha autorizados para fazer login no console de manutenção do servidor Unified Manager.

O problema de as coletas de estatísticas de desempenho não serem concluídas a tempo 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 nas coletas de estatísticas. Não altere essa 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 que o Unified Manager relata. Por exemplo, os limites de desempenho definidos pelo sistema acionam eventos quando a política é excedida por 30 minutos. Ao usar coletas a cada 5 minutos, a política deve ser excedida por seis coletas consecutivas. Para coletas a cada 15 minutos, a política deve ser excedida por apenas dois períodos de coleta.

Uma mensagem na parte inferior da página de Configuração do Cluster indica o intervalo atual de coleta de dados estatísticos.

Passos

1. Faça login usando SSH como usuário de manutenção no host do Unified Manager.

   Os avisos do console de manutenção do Unified Manager são exibidos.

2. Digite o número da opção de menu rotulada **Configuração do intervalo de sondagem de desempenho** e pressione Enter.
3. Caso seja solicitado, digite novamente a senha do usuário de manutenção.
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 ativa com um provedor de dados externo (como o Graphite), você deve alterar o intervalo de transmissão do provedor de dados para que ele seja igual ou maior que o intervalo de coleta do Unified Manager.

Solucione problemas de cargas de trabalho usando o analisador de carga de trabalho

Solucione problemas de cargas de trabalho com o analisador de cargas de trabalho no Active IQ Unified Manager

O analisador de carga de trabalho permite visualizar critérios importantes de integridade e desempenho para uma única carga de trabalho em uma única página para auxiliar na resolução 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 ela pode estar apresentando problemas de desempenho ou capacidade no momento.

O uso desta ferramenta também pode ajudar você a determinar se o armazenamento é a causa de algum problema de desempenho de um aplicativo ou se o problema é causado pela rede ou por outro problema relacionado.

Você pode iniciar essa funcionalidade em diversos locais da interface de usuário:

- Na seleção Workload Analysis no menu de navegação à esquerda
- Na página de detalhes do evento, clique 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), clique no ícone Mais e, em seguida, em **Analyze Workload**

- Na página Virtual Machines, clicando no botão **Analyze Workload** em qualquer objeto Datastore

Ao iniciar a ferramenta pelo 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 inventário de carga de trabalho ou 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 pela página de detalhes do evento, o nome da carga de trabalho é preenchido automaticamente, e os dados de 10 dias são exibidos.

Compreenda os dados do analisador de carga de trabalho no Active IQ Unified Manager

A página do analisador de carga de trabalho exibe informações sobre quaisquer eventos atuais que possam estar afetando a carga de trabalho, recomendações para corrigir o problema que pode estar 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 para o qual deseja visualizar estatísticas. Você pode alterar o período a qualquer momento, caso queira visualizar um período 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 durante o período. Quando há eventos de diferentes áreas de impacto (por exemplo, desempenho e capacidade), essas informações são exibidas para que você possa selecionar os detalhes do tipo de evento de seu interesse. Clique no tipo de evento para visualizar uma lista com os nomes dos eventos.

  Se houver apenas um evento durante o período analisado, você verá uma lista de recomendações para corrigir o problema em alguns eventos.

- **Linha do tempo do evento**

  Exibe todas as ocorrências de eventos durante o período especificado. Passe o cursor sobre cada evento para visualizar 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 (tanto do nó quanto do agregado) com base no período selecionado. Você pode clicar no link "View performance details" para exibir a página do Performance Explorer da carga de trabalho, caso deseje realizar uma análise adicional.

  - **Latência** exibe a latência da carga de trabalho no período selecionado. O gráfico possui três visualizações que permitem ver:

- latência **total**
- **Detalhamento** da latência (dividida em leituras, gravações e outros processos)
- **Componentes do cluster** latência (discriminada por componente do cluster)

Consulte "Componentes de cluster e por que eles podem entrar em conflito" para ver uma descrição dos componentes do cluster exibidos aqui. **Taxa de transferência exibe a taxa de transferência em IOPS e MB/s da carga de trabalho no período selecionado. O gráfico tem quatro visualizações que permitem ver:** * taxa de transferência **total * taxa de transferência detalhada (separada por leituras, gravações e outros processos)** * **Taxa de transferência na nuvem** (os MB/s usados para gravar dados na nuvem e ler dados da nuvem, para as cargas de trabalho que fazem o tiering da capacidade para a nuvem) *** IOPS com previsão (uma previsão de quais valores superior e inferior da taxa de transferência em IOPS eram esperados no período) Este gráfico também exibe as configurações de limite máximo e mínimo de taxa de transferência da 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 em que a carga de trabalho está em execução no período selecionado. A partir daqui, você pode ver se seu agregado ou nó está com utilização excessiva, o que pode estar causando alta latência. Ao analisar volumes FlexGroup, há vários nós e vários agregados listados nos gráficos de utilização.

- **Área do gráfico de capacidade**

  Exibe gráficos da capacidade de dados e da capacidade de Snapshot 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 deseje realizar análises adicionais. LUNs não fornecem esse link porque não existe uma página "Detalhes de integridade" para LUNs.

  - A **Visualização de capacidade** exibe o espaço total disponível alocado para a carga de trabalho e o espaço lógico usado (após todas as otimizações da NetApp).
  - A **Snapshot View** exibe o espaço total reservado para cópias Snapshot e a quantidade de espaço em uso no momento. Observe que os LUNs não fornecem uma Snapshot View.
  - **Cloud Tier View** exibe quanta capacidade está sendo usada na camada de desempenho local e quanta está sendo usada na camada de nuvem. Esses gráficos incluem uma estimativa do tempo restante até que a capacidade fique cheia para essa carga de trabalho. Essas informações se baseiam no histórico de uso e exigem um mínimo de 10 dias de dados. Quando restam menos de 30 dias de capacidade, o Unified Manager identifica o armazenamento como “almost full”.

Entenda quando usar o analisador de carga de trabalho no Active IQ Unified Manager

Normalmente, você usaria o analisador de carga de trabalho para solucionar um problema de latência relatado por um usuário, para analisar mais detalhadamente um evento ou alerta relatado ou para explorar uma carga de trabalho que você considera estar operando de forma anormal.

No caso de os usuários entrarem em contato com você para dizer que o aplicativo que estão usando está muito lento, você pode verificar os gráficos de latência, throughput e utilização da carga de trabalho na qual o aplicativo está sendo executado para ver se o storage é a causa do problema de desempenho. Você também pode usar o gráfico de capacidade para ver se a capacidade está baixa, porque um sistema ONTAP com mais de 85% da capacidade em uso pode causar problemas de desempenho. Esses gráficos ajudarão você a determinar se o problema é causado pelo storage, 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 de detalhes do evento clicando no botão **Analyze Workload** para pesquisar algumas das tendências de latência, taxa de transferência e capacidade da carga de trabalho.

Caso você note uma carga de trabalho que pareça estar operando de forma anormal ao visualizar qualquer página de inventário de cargas de trabalho (volume, LUN, carga de trabalho, compartilhamento NFS ou compartilhamento SMB/CIFS), você pode clicar no ícone Mais , depois em **Analyze Workload** para abrir a página de análise de carga de trabalho e examinar melhor a carga de trabalho.

Utilize o analisador de carga de trabalho no Active IQ Unified Manager

Existem várias maneiras de iniciar o analisador de carga de trabalho a partir da interface de usuário. Aqui descrevemos como iniciar a ferramenta a partir do painel de navegação à esquerda.

Passos

1. No painel de navegação esquerdo, clique em **Análise de carga de trabalho**.

   A página de Análise de Carga de Trabalho é exibida.

2. Se você souber o nome da carga de trabalho, digite-o. Caso não tenha certeza do nome completo, digite 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 desejar visualizar estatísticas por mais de 2 horas, o padrão, e clique em **Apply**.
4. Consulte a área Summary para ver os eventos que ocorreram durante o período.
5. Consulte os gráficos de desempenho e capacidade para verificar quando alguma das métricas apresentar anormalidades e veja se algum evento coincide com o registro anormal.

Monitore o desempenho do cluster na Performance Cluster Landing page

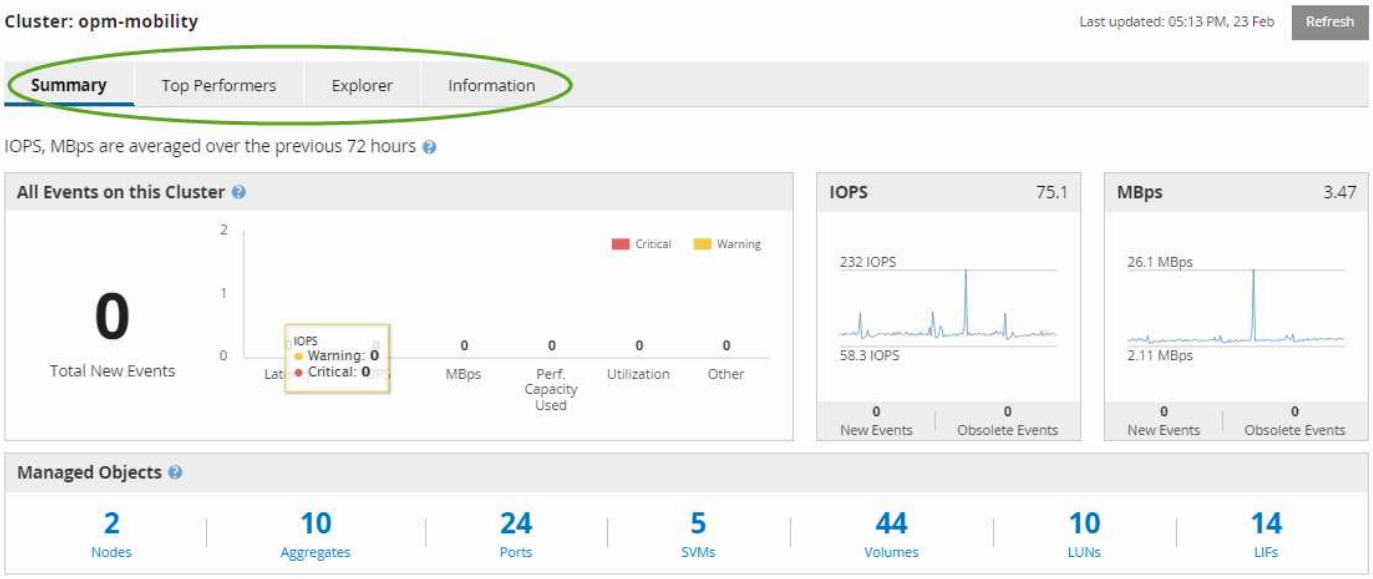
Monitore o desempenho do cluster na página inicial de desempenho do cluster no Active IQ Unified Manager

A página de destino do cluster de desempenho exibe o status de desempenho de alto nível de um cluster selecionado que está sendo monitorado por uma instância do Unified Manager. Esta página permite que você avalie o desempenho geral de um cluster específico e registre, localize ou atribua rapidamente para resolução quaisquer eventos específicos do cluster que forem identificados.

Entenda a página inicial do Cluster de Desempenho no Active IQ Unified Manager

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. Os 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 a você informações sobre eventos e desempenho e permite monitorar e solucionar problemas dos clusters. A imagem a seguir mostra um exemplo da página inicial do cluster de desempenho para o cluster chamado opm-mobility:



A contagem de eventos na página Resumo do Cluster pode não corresponder à contagem de eventos na página Inventário de Eventos de Desempenho. Isso ocorre porque a página Resumo do Cluster pode exibir um evento em cada uma das barras de Latência e Utilização quando as políticas de limite de combinação são violadas, enquanto a página Inventário de Eventos de Desempenho exibe apenas um evento quando uma política de combinação é violada.

Se um cluster for removido do gerenciamento do Unified Manager, o status **Removido** será exibido à direita do nome do cluster, na parte superior da página.

Página inicial do cluster de desempenho

Analise a página inicial do Cluster de Desempenho no Active IQ Unified Manager

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 dos objetos de armazenamento no cluster selecionado.

A página inicial do cluster de desempenho inclui quatro abas que separam os detalhes do cluster em quatro áreas de informação:

- Página de resumo
  - Painel de eventos do cluster
  - Gráficos de desempenho em MB/s e IOPS
  - Painel de Objetos Gerenciados
- Página dos Melhores Desempenhos
- Página do explorador
- Página de informações

Página de resumo do cluster de desempenho

Consulte a página de Resumo do Cluster de Desempenho em Active IQ Unified Manager

A página Resumo do Desempenho do Cluster fornece um resumo dos eventos ativos, do desempenho de IOPS e do desempenho em MB/s de um cluster. Esta página também inclui a contagem total dos objetos de armazenamento no cluster.

Analise o painel de eventos de desempenho do cluster no Active IQ Unified Manager

O painel de 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 os eventos relacionados ao cluster.

Painel Todos os eventos deste cluster

O painel "Todos os Eventos neste Cluster" exibe todos os eventos de desempenho ativos do cluster nas últimas 72 horas. O "Total de Eventos Ativos" é exibido na extremidade esquerda; esse número representa o total de todos os eventos Novos e Confirmados de todos os objetos de armazenamento neste cluster. Você pode clicar no link "Total de Eventos Ativos" para ir para a página "Inventário de Eventos", filtrada para exibir esses eventos.

O gráfico de barras "Total de Eventos Ativos" para o cluster exibe o número total de eventos críticos e de aviso ativos:

- Latência (total para os 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)
- Outro (taxa de falha de cache para volumes)

A lista contém eventos de desempenho ativos acionados por políticas de limiar definidas pelo usuário, políticas de limiar definidas pelo sistema e limiares dinâmicos.

Os dados do gráfico (barras verticais do contador) são exibidos em vermelho (🟥) para eventos críticos e em amarelo (🟨) para eventos de aviso. Posicione o cursor sobre cada barra vertical do contador para visualizar o tipo e o número reais de eventos. Você pode clicar em **Refresh** para atualizar os dados do painel do contador.

Você pode exibir ou ocultar eventos críticos e de aviso no gráfico de desempenho "Total Active Events" clicando nos ícones **Critical** e **Warning** na legenda. Se você ocultar determinados tipos de eventos, os ícones da legenda serão exibidos em cinza.

Painéis de contadores

Os painéis de contadores exibem a atividade do cluster e os eventos de desempenho das últimas 72 horas e incluem os seguintes contadores:

- **Painel de contador de 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 de 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 de IOPS em um horário específico.

- **Painel do contador de MB/s**

  MB/s indica a quantidade de dados transferidos de e para o cluster em megabytes por segundo. Este painel de contadores 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 em um horário específico.

O número no canto superior direito do gráfico na barra cinza representa o valor médio das últimas 72 horas. Os números exibidos na parte inferior e superior do gráfico de linha de tendência representam os valores mínimo e máximo das últimas 72 horas. A barra cinza abaixo do gráfico contém a contagem de eventos ativos (novos e confirmados) e eventos obsoletos das últimas 72 horas.

Os painéis de contadores contêm dois tipos de eventos:

- **Ativo**

  Indica que o evento de desempenho está atualmente ativo (novo ou reconhecido). O problema que causou o evento não foi corrigido ou 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 se corrigiu sozinho ou foi resolvido. O contador de desempenho do objeto de armazenamento não está mais acima do limite de desempenho.

Para **Eventos Ativos**, se houver apenas um evento, você pode posicionar o cursor sobre o ícone do evento e clicar no número do evento para acessar a página de Detalhes do Evento correspondente. Se houver mais de um evento, você pode clicar em **Ver todos os Eventos** para exibir a página de Inventário de Eventos, filtrada para mostrar todos os eventos do tipo de contador de objeto selecionado.

Analise o painel Objetos Gerenciados no Active IQ Unified Manager

O painel Objetos Gerenciados na guia Resumo de Desempenho fornece uma visão geral de alto nível dos tipos e das 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 é um dado de ponto no tempo referente ao último período de coleta. Novos objetos são descobertos em intervalos de 15 minutos.

Ao clicar no número vinculado de qualquer tipo de objeto, você verá a página de inventário de desempenho desse 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 múltiplos grupos de redundant array of independent disks (RAID) que podem ser gerenciados como uma única unidade para proteção e provisionamento.

- **Portas**

  Um ponto de conexão física nos nós que é usado para se 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 a partir de um namespace distinto e é administrável separadamente do restante do cluster.

- **Volumes**

  Uma entidade lógica que mantém dados de usuário acessíveis por meio de um ou mais protocolos de acesso compatíveis. A contagem inclui volumes FlexVol e volumes FlexGroup; não inclui constituintes de FlexGroup.

- **LUNs**

  O identificador de uma unidade lógica Fibre Channel (FC) ou de uma unidade lógica iSCSI. Uma unidade lógica normalmente corresponde a um volume de armazenamento e é representada em um sistema operacional como um dispositivo.

- **Interfaces de rede**

  Uma interface de rede lógica que representa um ponto de acesso à rede para um nó. A contagem inclui todos os tipos de interface.

Veja a página dos Melhores Desempenhos em Active IQ Unified Manager

A página "Melhores Desempenhos" exibe os objetos de storage que têm o maior desempenho ou o menor desempenho, com base no contador de desempenho que você selecionar. Por exemplo, na categoria "VMs de storage", você pode exibir as SVMs que têm o maior número de IOPS, a maior latência ou o menor MB/s. Esta página também mostra se algum dos objetos com melhor desempenho tem eventos de desempenho ativos (novos ou reconhecidos).

A página "Top Performers" exibe no máximo 10 de cada objeto. Observe que o objeto "Volume" inclui tanto volumes FlexVol quanto volumes FlexGroup.

- **Período de tempo**

  Você pode selecionar um intervalo de tempo para visualizar os itens com melhor desempenho; o intervalo de tempo selecionado se aplica a todos os objetos de storage. 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 de cada 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 objetos de melhor desempenho com base no contador selecionado.

Contadores disponíveis:

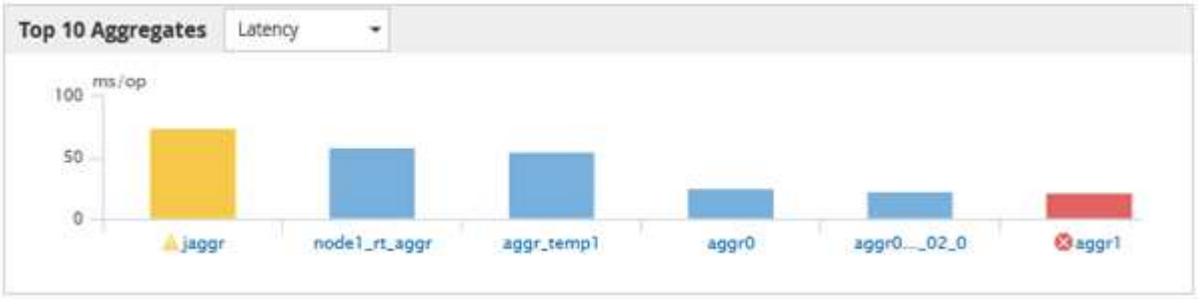
- Latência
- IOPS
- MB/s
- Capacidade de desempenho utilizada (para nós e agregados)
- Utilização (para nós e agregados)

- **Ordenar**

Clique no menu **Classificar** para selecionar uma classificação crescente ou decrescente para o objeto e o contador selecionados. As opções são **Do maior para o menor** e **Do menor para o maior**. Essas opções permitem visualizar os objetos com o maior desempenho ou o menor desempenho.

- **Barra de contador**

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 estiver ultrapassando 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 são exibidos em amarelo ( ) e eventos críticos são exibidos em vermelho ( ). As violações de limite também são indicadas por ícones indicadores de gravidade do evento para eventos de aviso e críticos.



Em cada gráfico, o eixo X exibe os itens com melhor desempenho para o tipo de objeto selecionado. O eixo Y exibe as unidades aplicáveis ao contador selecionado. Clicar no link do nome do objeto abaixo de cada elemento do gráfico de barras vertical leva você à página inicial de desempenho do objeto selecionado.

- **Indicador de evento de severidade**

O ícone indicador de **Evento Grave** é exibido à esquerda do nome de um objeto para eventos críticos ativos ( ) ou de aviso ( ) nos gráficos de melhor desempenho. Clique no ícone indicador de **Evento Grave** para visualizar:

- **Um evento**

  Leva você à página de detalhes desse evento.

- **Dois ou mais eventos**

  Navega até a página de inventário de eventos, filtrada para exibir todos os eventos do objeto selecionado.

- **Botão Exportar**

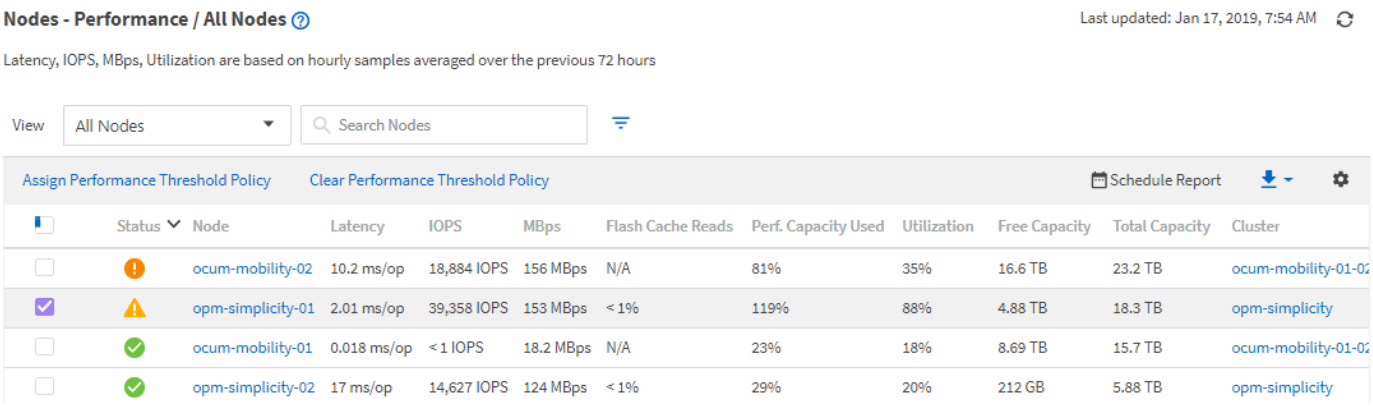
  Cria um `.csv` arquivo que contém os dados exibidos na barra de contagem. Você pode optar por criar o arquivo para o cluster específico que está visualizando ou para todos os clusters do data center.

Monitore o desempenho usando as páginas de Inventário de Desempenho

Monitore o desempenho de objetos usando as páginas de Inventário de Desempenho no Active IQ Unified Manager

As páginas de desempenho do inventário de objetos exibem informações de desempenho, eventos de desempenho e integridade dos objetos para todos os objetos em uma categoria de tipo de objeto. Isso fornece a você uma visão geral rápida do status de desempenho de cada objeto em 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 dos objetos, permitindo que você avalie o desempenho geral de todos os objetos e compare os dados de desempenho dos objetos. Você pode refinar o conteúdo das páginas de inventário de objetos pesquisando, classificando e filtrando. Isso é útil para monitorar e gerenciar o desempenho dos objetos, pois permite que você localize rapidamente objetos com problemas de desempenho e inicie o processo de solução de problemas.



Por padrão, os objetos nas páginas de inventário de desempenho são classificados com base na criticidade do desempenho do objeto. Os objetos com novos eventos críticos de desempenho aparecem primeiro, e os objetos com eventos de aviso aparecem em segundo lugar. Isso fornece uma indicação visual imediata dos problemas que precisam ser resolvidos. Todos os dados de desempenho se baseiam 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 Performance/All Nodes, você clicaria em um objeto de nó na coluna **Nodes**. A página de detalhes do objeto fornece informações detalhadas sobre o objeto selecionado, incluindo uma comparação lado a lado

dos eventos ativos.

Visualize as páginas de inventário de desempenho para todos os objetos de storage no Active IQ Unified Manager

Você usa as páginas de inventário de desempenho para ver um resumo das informações de desempenho de cada um dos objetos de armazenamento disponíveis, como clusters, agregados, volumes e assim por diante. Você pode acessar as páginas de detalhes do objeto de desempenho para visualizar informações detalhadas de um objeto específico.

Por padrão, os objetos nas páginas de visualização são classificados com base na criticidade do evento. Os objetos com eventos críticos são listados primeiro, e os objetos com eventos de aviso são listados em segundo lugar. Isso fornece uma indicação visual imediata dos problemas que precisam ser resolvidos.

Você pode exportar dados destas páginas para um arquivo de valores separados por vírgula (`.csv`), um arquivo do Microsoft Excel (`.xlsx`) ou um documento (`.pdf`) usando o botão **Relatórios** e, em seguida, usar os dados exportados para criar relatórios. Além disso, você pode personalizar a página e agendar a criação e o envio de um relatório por e-mail regularmente usando o botão **Relatórios Agendados**.

Todos os campos destas páginas podem ser usados em visualizações personalizadas e em relatórios. Alguns campos estão vinculados a páginas relacionadas permitindo uma visualização mais detalhada.

Desempenho: visualização de todos os clusters

A visualização Performance: All Clusters exibe uma visão geral dos eventos de desempenho, dos dados e das informações de configuração de cada cluster monitorado por uma instância do Unified Manager. Esta página permite que você monitore o desempenho dos seus clusters e solucione problemas de desempenho e eventos de limite.

Você pode atribuir políticas de limite de desempenho ou remover políticas de limite de desempenho de qualquer objeto nas páginas de inventário de objetos usando os botões **Atribuir Política de Limite de Desempenho** e **Remover Política de Limite de Desempenho**.

A seguir, apresentamos alguns campos importantes na visualização 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) da LIF de gerenciamento do cluster.
- Versão do SO: a versão do software ONTAP que está instalada no cluster.

> Se diferentes versões do software ONTAP estiverem instaladas nos nós do cluster, o número da versão mais baixa será listado. Você pode ver a versão do ONTAP instalada em cada nó na visualização Performance: All Nodes.

- Política de limite: a política de limite de desempenho definida pelo usuário, ou políticas, que estão ativas neste objeto de armazenamento. Você pode posicionar o cursor sobre nomes de políticas que contêm reticências (…) para visualizar o nome completo da política ou a lista de nomes de políticas atribuídas. Os botões Atribuir Política de Limite de Desempenho e Limpar Política de Limite de Desempenho

permanecem desativados até que você selecione um ou mais objetos clicando nas caixas de seleção localizadas na extremidade esquerda.

Desempenho: visualização de todos os volumes

A visualização Desempenho: Todos os Volumes exibe uma visão geral dos eventos de desempenho, dos dados de contador e das informações de configuração para cada FlexVol volume e FlexGroup volume 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 de mais opções ⋮ e, em seguida, em **Analyze Workload**, e você poderá visualizar gráficos de desempenho e capacidade na página Workload Analysis. Você pode visualizar os detalhes no System Manager, desde que tenha credenciais válidas para o System Manager.

ⓘ Para volumes de proteção de dados (DP), apenas os valores de contador para o tráfego gerado pelo usuário são exibidos. Os volumes raiz não são exibidos nesta página.

A seguir, apresentamos alguns campos importantes na visualização Desempenho: todos os volumes.

- Estilo: ou FlexVol ou FlexGroup.
- Latência: para volumes FlexVol, este é o tempo de resposta médio 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 consumido pela carga de trabalho, em terabytes. Este contador mede o desempenho que pode ser obtido com uma determinada capacidade de storage.
- IOPS: para volumes FlexVol, este é o número de operações de entrada/saída por segundo do volume. Para volumes FlexGroup, esta é a soma dos IOPS de todos os volumes constituintes.
- MB/s: para FlexVol volumes, esta é a taxa de transferência no volume, medida em megabytes por segundo. Para FlexGroup volumes, esta é a soma de MB/s de todos os volumes constituintes.
- Campos de capacidade: capacidade livre e total em GiB.

Consulte os seguintes links para obter 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"
- "Entendendo as recomendações do Unified Manager para hierarquizar dados na nuvem"
- "Visualizar gráficos de desempenho para comparar volumes ou LUNs que estejam no mesmo grupo de política de QoS"

Desempenho: visualização de todos os agregados

A visualização Performance: All Aggregates 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, apresentamos 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 está ativado.
  - Híbrido (Flash Pool). Combina HDDs e SSDs, e o Flash Pool está ativado.
  - SSD
  - SSD (FabricPool). Combina SSDs e uma camada de nuvem
  - HDD (FabricPool). Combina HDDs e uma camada de nuvem
  - VMDisk (SDS). Discos virtuais em uma máquina virtual
  - VMDisk (FabricPool). Combina discos virtuais e um tier de nuvem
  - LUN
- Relatório de Dados Inativos: indica se o recurso de relatório de dados inativos está habilitado ou desabilitado neste agregado. Quando habilitado, os volumes neste agregado exibem a quantidade de dados frios na visualização Performance: All Volumes. O valor neste campo é "N/A" quando a versão do ONTAP não oferece suporte ao relatório de dados inativos.
- Política de limite: a política de limite de desempenho definida pelo usuário, ou políticas, 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 "Assign Performance Threshold Policy" e "Clear Performance Threshold Policy" permanecem desativados até que você selecione um ou mais objetos clicando nas caixas de seleção localizadas na extremidade esquerda. Consulte os links a seguir para obter 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 visualização 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 atendidas pelo cache, em vez de serem retornadas do disco. Os dados do Flash Cache são exibidos apenas para nós e somente quando um módulo Flash Cache está instalado no nó.

No menu **Relatórios**, a opção **Relatório de Inventário de Hardware** é disponibilizada quando o Unified Manager e os clusters que ele gerencia estão 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 dos nós, como números de modelo e de série do hardware, tipos e quantidades de discos, licenças instaladas e muito mais. Essa funcionalidade de relatório é útil para a renovação de contratos em sites seguros que não estão conectados à plataforma NetApp Active IQ. Você pode atribuir políticas de limite de desempenho a qualquer objeto nas páginas de inventário de objetos ou remover essas políticas usando os botões **Atribuir Política de Limite de Desempenho** e **Remover Política de Limite de Desempenho**.

Consulte os seguintes links para obter mais informações:

- "Atribuindo políticas de limite de desempenho a objetos de armazenamento"

- "Removendo políticas de limite de desempenho de objetos de armazenamento"
- "Geração de um relatório de inventário de hardware para renovação de contrato"

Desempenho: visualização de todas as VMs de armazenamento

A visualização Performance: All Storage VMs exibe uma visão geral dos eventos de desempenho, dos dados e das informações de configuração de cada máquina virtual de storage (SVM) que está sendo monitorada por uma instância do Unified Manager. Isso permite que você monitore rapidamente o desempenho das suas SVMs e solucione problemas de desempenho e eventos de limite. O campo Latência nesta página informa o tempo de resposta médio de todas as solicitações de E/S, expresso em milissegundos por operação.



As SVMs listadas nesta página incluem apenas SVMs de dados e de cluster. O Unified Manager não usa nem exibe SVMs de administração ou de nó.

Consulte os seguintes links para obter 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 visualização Desempenho: todas as LUNs exibe uma visão geral dos eventos de desempenho, dados e informações de configuração para cada LUN que está sendo monitorada por uma instância do Unified Manager. Isso permite que você monitore rapidamente o desempenho de suas 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 ⋮, depois em **Analyze Workload**, e você poderá visualizar gráficos de desempenho e capacidade na página **Workload Analysis**.

Consulte os seguintes links para obter 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"
- "Visualizando volumes ou LUNs que estão no mesmo grupo de políticas 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 visualização 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, além de solucionar 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 de NVRAM. *

Erro de espaço - o Namespace ficou sem espaço.

Consulte os seguintes links para obter 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 visualização Desempenho: todas as interfaces de rede exibe uma visão geral dos eventos de desempenho, dados e informações de configuração de cada interface de rede (LIF) que está sendo monitorada por esta instância do Unified Manager. Esta página permite que você monitore rapidamente o desempenho das suas interfaces e solucione problemas de desempenho e eventos de limite. A seguir, estão alguns campos importantes na visualização Desempenho: todas as interfaces de rede.

- IOPS: operações de entrada/saída por segundo. IOPS não se aplica a LIFs NFS e LIFs CIFS, e é exibido como N/A para esses tipos.
- Latência: o tempo médio de resposta para todas as solicitações de E/S, expresso em milissegundos por operação. A latência não se aplica a LIFs NFS e LIFs CIFS e é exibida como N/D para esses tipos.
- Localização inicial: a localização inicial da interface, exibida como nome do nó e nome da porta, separados por dois pontos (:). Se a localização for exibida com reticências (…), você pode posicionar o cursor sobre o nome da localização para visualizar a localização completa.
- Localização atual: a localização atual da interface, exibida como nome do nó e nome da porta, separados por dois pontos (:). Se a localização for exibida com reticências (…), você pode posicionar o cursor sobre o nome da localização para visualizar a localização completa.
- 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 de sistema.

Desempenho: visualização de todas as portas

A visualização Desempenho: todas as portas exibe uma visão geral dos eventos de desempenho, dos dados e das informações de configuração de cada porta que está sendo monitorada por uma instância do Unified Manager. Isso permite que você monitore rapidamente o desempenho das suas portas e solucione problemas de desempenho e eventos de limite. Para a função de uma porta, a função da porta de rede é exibida como Data ou Cluster. As portas FCP não podem ter uma função e a função é exibida como N/A.

Os valores dos contadores de desempenho são exibidos apenas para portas físicas. Os valores dos contadores não são exibidos para VLANs ou grupos de interfaces.

Consulte os seguintes links para obter mais informações:

- "Atribuindo políticas de limite de desempenho a objetos de armazenamento"
- "Removendo políticas de limite de desempenho de objetos de armazenamento"

Desempenho: visão dos grupos de políticas de QoS

A visualização Grupos de políticas de QoS exibe os grupos de políticas de QoS disponíveis nos clusters que o Unified Manager está monitorando. Isso inclui políticas de QoS tradicionais, políticas de QoS adaptáveis e

políticas de QoS atribuídas usando Performance Service Levels.

A seguir, apresentamos alguns campos importantes na visualização Desempenho: grupos de políticas de QoS.

- Grupo de políticas de QoS: o nome do grupo de políticas de QoS. Para políticas do NetApp Service Level Manager (NSLM) 1.3 que foram importadas para o Unified Manager 9.7 ou superior, o nome exibido aqui inclui o nome da SVM e outras informações que não constam no nome quando o Nível de Serviço de Desempenho foi definido no NSLM. Por exemplo, o nome "NSLM_vs6_Performance_2_0" significa que esta é a política PSL "Performance" definida pelo sistema NSLM, criada na SVM "vs6" com uma latência esperada de "2 ms/op".
- SVM: a máquina virtual de storage (SVM) à qual o grupo de políticas de QoS pertence. Você pode clicar no nome da máquina virtual de storage para navegar até a página de detalhes dessa máquina virtual de storage. Observe que este campo fica em branco se a política de QoS tiver sido criada na máquina virtual de storage Admin, pois esse tipo de máquina virtual de storage representa o cluster.
- Taxa de transferência mínima: a taxa de transferência mínima, em IOPS, que o grupo de políticas garantirá fornecer. Para políticas adaptáveis, este é o mínimo de IOPS esperado por TB alocado ao volume ou à LUN, com base no tamanho alocado do objeto de storage.
- Taxa de transferência máxima: a taxa de transferência, em IOPS e/ou MB/s, que o grupo de políticas não deve exceder. Quando este campo estiver em branco, significa que a taxa de transferência máxima definida no ONTAP é infinita. Para políticas adaptáveis, este é o máximo (pico) possível de IOPS por TB alocado ao volume ou LUN, com base no tamanho alocado ou no tamanho usado do objeto de armazenamento.
- IOPS mínimo absoluto: para políticas adaptáveis, este é o valor mínimo absoluto de IOPS usado como substituição quando o IOPS esperado for menor que esse valor.
- Tamanho do bloco: o tamanho do bloco especificado para a política adaptável de QoS.
- Alocação mínima: indica se o "espaço alocado" ou o "espaço utilizado" é usado para determinar a taxa de transferência máxima (pico) de IOPS.
- Latência esperada: a latência média esperada para operações de entrada/saída de storage.
- Compartilhado: para políticas de QoS tradicionais, indica se os valores de throughput 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 de expansão ( ) ao lado do nome do grupo de políticas de QoS para visualizar mais detalhes sobre o grupo de políticas.
- Capacidade alocada: a quantidade de espaço que os objetos no grupo de política de QoS estão utilizando atualmente.
- 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 obter mais informações consulte os tópicos em "Gerenciar o desempenho usando informações do grupo de políticas de QoS".

Conteúdo da página de inventário do Refine Performance

Aprimore o conteúdo da página de inventário de desempenho em Active IQ Unified Manager

As páginas de inventário de objetos de desempenho contêm ferramentas para ajudar você a refinar o conteúdo dos dados de inventário de objetos, permitindo localizar 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 aprimorar o desempenho; no entanto, localizar dados específicos requer ferramentas que permitam encontrá-los rapidamente. Portanto, as páginas de inventário de objetos de desempenho incluem funcionalidades de busca, classificação e filtragem. Além disso, a busca e a filtragem podem ser combinadas para refinar ainda mais os resultados.

Pesquise nas páginas de desempenho do inventário de objetos em Active IQ Unified Manager

Você pode pesquisar cadeias de caracteres nas páginas de Desempenho do Inventário de Objetos. Use o campo **Pesquisar** localizado no canto superior direito da página para encontrar rapidamente dados com base no nome do objeto ou no nome da política. Isso permite localizar rapidamente objetos específicos e seus dados associados, ou localizar rapidamente políticas e visualizar os dados associados dos objetos de política.

Etapa

1. Execute uma das seguintes opções, com base nos seus requisitos de busca:

Para localizar isso…	Digite isto…
Um objeto específico	Insira o nome do objeto no campo **Pesquisar** e clique em **Pesquisar**. O objeto pesquisado e seus dados relacionados são exibidos.
Uma política de limite de desempenho definida pelo usuário	Digite o nome da política, total ou parcialmente, no campo **Pesquisar** e clique em **Pesquisar**. Os objetos atribuídos à política que você pesquisou são exibidos.

Classifique os dados nas páginas de desempenho do inventário de objetos no Active IQ Unified Manager

Você pode classificar todos os dados nas páginas de Desempenho do Inventário de Objetos por qualquer coluna, em ordem crescente ou decrescente. Isso permite localizar rapidamente os dados do inventário de objetos, o que é útil ao analisar o desempenho ou iniciar um processo de solução de problemas.

A coluna selecionada para ordenação é indicada por um nome de cabeçalho de coluna destacado e um ícone de seta à direita do nome, que indica a direção da ordenação. Uma seta para cima indica ordem crescente; uma seta para baixo indica ordem decrescente. A ordem de ordenação 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.

Filtre os dados nas páginas de desempenho do inventário de objetos no Active IQ Unified Manager

Você pode filtrar os dados nas páginas de Desempenho do Inventário de Objetos para localizar rapidamente os dados com base em critérios específicos. Você pode usar a filtragem para restringir o conteúdo das páginas de Desempenho do Inventário de Objetos e exibir apenas os resultados que você especificou. Isso proporciona um método muito eficiente para exibir somente os dados de desempenho que interessam a você.

Você pode usar o painel de filtragem para personalizar a visualização em grade de acordo com suas preferências. As opções de filtro disponíveis dependem do tipo de objeto que está sendo visualizado na grade. Se houver filtros aplicados, o número de filtros aplicados será exibido à direita do botão Filtrar.

Há suporte para três tipos de parâmetros de filtro.

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**.

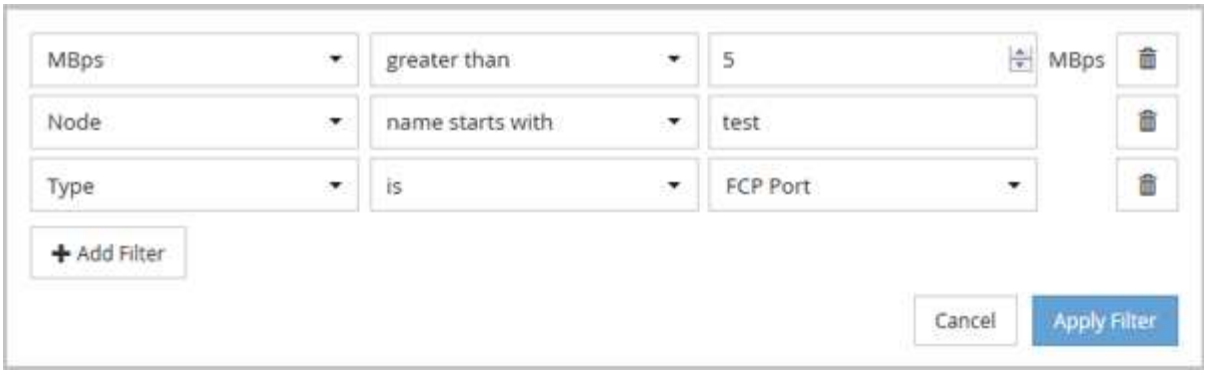
Os campos Coluna, Operador e Valor são obrigatórios para cada filtro; os filtros disponíveis refletem as colunas filtráveis na página atual. O número máximo de filtros que você pode aplicar é quatro. Os resultados filtrados são baseados na combinação dos parâmetros de filtro. Os resultados filtrados se aplicam a todas as páginas da sua pesquisa filtrada, não apenas à página exibida no momento.

Você pode adicionar filtros usando o painel de Filtragem.

1. Na parte superior da página, clique no botão **Filtrar**. O painel de 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 desse objeto.
5. Para adicionar outro filtro, clique em **+Add Filter**. Um campo de filtro adicional é exibido. Preencha este filtro usando o processo descrito nas etapas anteriores. Observe que, ao adicionar o seu quarto filtro, o botão **+Add Filter** não é 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 de filtragem para remover filtros individuais clicando no ícone da lixeira à direita do filtro que você deseja remover.
8. Para remover todos os filtros, clique em **Reset** na parte inferior do painel de filtragem.

Exemplo de filtragem

A ilustração mostra o painel de filtragem com três filtros. O botão **+Adicionar Filtro** é exibido quando você tem menos de quatro filtros, o limite máximo.



Após clicar em **Aplicar filtro**, o painel de filtragem fecha, aplica seus filtros e mostra o número de filtros aplicados (3).

Analise as recomendações do Active IQ Unified Manager para o armazenamento em camadas de dados na nuvem

A visualização Performance: All Volumes exibe informações relacionadas ao tamanho dos dados de usuário armazenados no volume que está inativo (frio). Em alguns casos, o Unified Manager identifica determinados volumes que se beneficiariam com a disposição em camadas dos dados inativos para a camada de nuvem (provedor de nuvem ou o 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 fazer o armazenamento em camadas dos dados exige que você atualize o software ONTAP. Além disso, a **`auto`** política de armazenamento em camadas foi introduzida no ONTAP 9.4, e a **`all`** política de armazenamento em camadas foi introduzida no ONTAP 9.6, portanto, se a recomendação for usar a política de armazenamento em camadas automática, você deverá atualizar para o ONTAP 9.4 ou superior.

Os três campos a seguir na visualização Performance: All Volumes fornecem informações sobre se você pode melhorar a utilização de disco do seu sistema de storage e economizar espaço na camada de desempenho movendo dados inativos para a camada de nuvem.

- **Política de disposição em camadas**

  A política de hierarquização determina se os dados no volume permanecem na camada de desempenho ou se parte dos dados é movida da camada de desempenho para a camada de nuvem.

  O valor neste campo indica a política de hierarquização definida no volume, mesmo que o volume não esteja atualmente em um agregado FabricPool. A política de hierarquização só entra em vigor quando o volume está em um agregado FabricPool.

- **Dados frios**

  Os dados frios exibem o tamanho dos dados de usuário armazenados no volume que está inativo (frio).

  Um valor é exibido aqui somente ao usar o software ONTAP 9.4 ou superior, pois isso requer que o agregado no qual o volume está implantado tenha o **`inactive data reporting parameter`** definido como **`enabled`**, e que o limite mínimo do número de dias de resfriamento tenha sido atingido (para

volumes que usam a política de tiering **snapshot-only** ou **auto**). Caso contrário, o valor aparece como "N/A".

- **Recomendação de nuvem**

  Após a coleta de informações suficientes sobre a atividade de dados no volume, o Unified Manager pode determinar que nenhuma ação é necessária ou que você pode economizar espaço na camada de desempenho movendo os dados inativos para a camada de nuvem.

> O campo Dados Frios é atualizado a cada 15 minutos, enquanto o campo Recomendação na 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 na Nuvem exibe a data em que a análise foi executada.

Quando o Inactive Data Reporting está ativado, o campo Cold Data 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 Cold Data nesse caso, mas é exibida quando você passa o cursor sobre a palavra **Tier** para visualizar a recomendação de nuvem.

As recomendações de nuvem que você verá são:

- **Aprendendo**. 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 primeiro o volume para um agregado habilitado para FabricPool. Em outros casos, quando o volume já está em um agregado FabricPool, basta alterar a política de categorização em camadas.
- **Nenhuma ação**. Ou o volume tem poucos dados inativos, o volume já está configurado com a política de armazenamento em camadas "auto" em um agregado do FabricPool, ou o volume é um volume de proteção de dados. Esse valor também é exibido quando o volume está offline ou quando está sendo usado em uma configuração do MetroCluster.

Para mover um volume, alterar a política de hierarquização de volume ou as configurações de relatório de dados inativos do agregado, use o ONTAP System Manager, os comandos da ONTAP CLI ou uma combinação dessas ferramentas.

Se você estiver conectado ao Unified Manager com a função Application Administrator ou Storage Administrator, o link **Configure Volume** estará disponível na recomendação na nuvem ao posicionar o cursor sobre a palavra **Tier**. Clique neste botão para abrir a página Volumes no System Manager e fazer a alteração recomendada.

Monitore o desempenho usando as páginas do Explorador de Desempenho

Monitore o desempenho usando as páginas do Performance Explorer no Active IQ Unified Manager

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.

Utilize objetos raiz para monitoramento de desempenho no Active IQ Unified Manager

O objeto raiz serve como base de comparação para outros objetos. Isso permite visualizar e comparar os dados de outros objetos com o objeto raiz, fornecendo análises de desempenho que auxiliam na solução de problemas e na melhoria do desempenho dos objetos.

O nome do objeto raiz é exibido na parte superior do painel Comparação. Os 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, apenas um objeto raiz é permitido. Os dados do objeto raiz são exibidos automaticamente nos gráficos do painel Gráficos de 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 do Volume Performance Explorer de Volume1, então Volume1 é o objeto raiz e não pode ser alterado. Se você quiser comparar com um objeto raiz diferente, deverá clicar no link de um objeto e abrir sua página inicial.

Eventos e limiares são exibidos apenas para objetos raiz.

Filtre objetos correlacionados na grade do Active IQ Unified Manager

A filtragem permite exibir um subconjunto menor e mais bem definido de objetos na grade. Por exemplo, se você tiver 25 volumes na grade, a filtragem permite visualizar apenas os volumes com taxa de transferência inferior a 90 MBps ou latência superior a 1 ms/op.

Especifique um intervalo de tempo para objetos correlacionados

Especifique um intervalo de tempo para objetos correlacionados no Active IQ Unified Manager

O seletor de intervalo de tempo na página Performance Explorer permite que você especifique o intervalo de tempo para a comparação de dados de objetos. Especificar um intervalo de tempo refina o conteúdo das páginas Performance Explorer para exibir apenas os dados de objetos dentro do intervalo de tempo especificado.

Refinar o intervalo de tempo oferece um método eficiente para exibir apenas os dados de desempenho que interessam a você. Você pode selecionar um intervalo de tempo predefinido ou especificar um intervalo personalizado. O intervalo de tempo padrão são as 72 horas anteriores.

Selecione um intervalo de tempo predefinido no Active IQ Unified Manager

Selecionar um intervalo de tempo predefinido é uma maneira rápida e eficiente de você personalizar e focar a saída de dados ao visualizar os dados de desempenho dos objetos do cluster. Ao selecionar um intervalo de tempo predefinido, os dados ficam disponíveis por até 13 meses.

Passos

1. No canto superior direito da página **Performance Explorer**, clique em **Time Range**.
2. No lado direito do painel **Seleção de Intervalo de Tempo**, selecione um intervalo de tempo predefinido.
3. Clique em **Aplicar intervalo**.

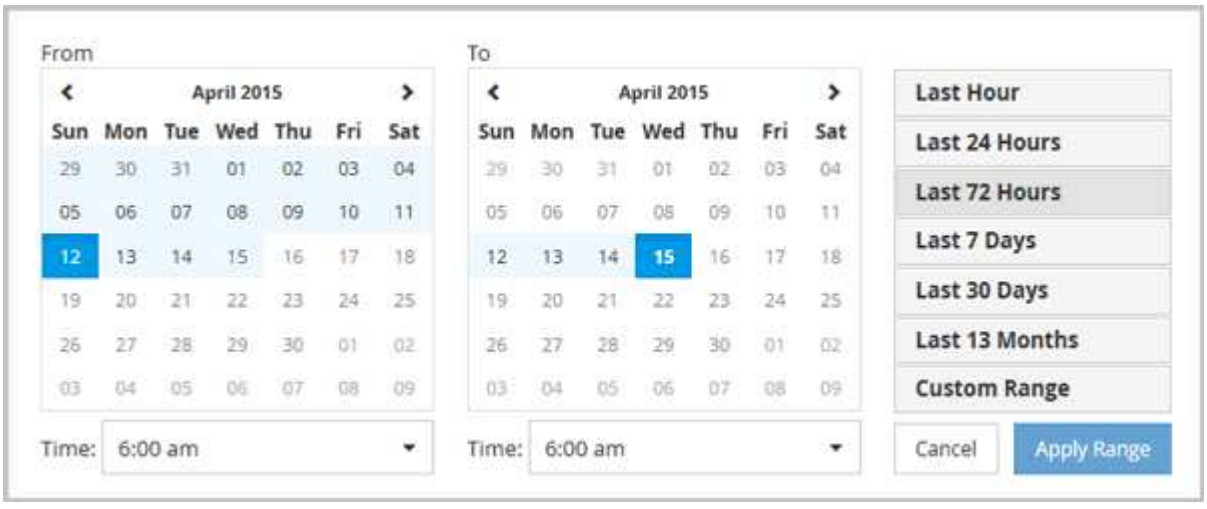
Especifique um intervalo de tempo personalizado no Active IQ Unified Manager

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 os dados do objeto do cluster.

Você pode selecionar um intervalo de tempo entre uma hora e 390 dias. Treze meses equivalem a 390 dias, pois 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 na solução de possíveis problemas de desempenho, pois especificar um intervalo de data e hora exibe com mais detalhes os dados ao redor do evento de desempenho. Use o controle **Intervalo de Tempo** para selecionar intervalos predefinidos de data e hora ou especifique seu próprio intervalo personalizado de data e hora de até 390 dias. Os botões de intervalos de tempo predefinidos variam de **Última Hora** a **Últimos 13 Meses**.

Selecionar a opção **Últimos 13 meses** ou especificar um intervalo de datas personalizado superior a 30 dias exibe uma caixa de diálogo alertando que os dados de desempenho exibidos para um período superior a 30 dias são apresentados em gráfico usando médias horárias, e não dados coletados a cada 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 será exibida quando você selecionar a opção **Últimos 13 meses** ou especificar um intervalo de datas personalizado superior a 30 dias. Os dados resumidos também se aplicam a um intervalo de tempo menor, se o intervalo de tempo incluir uma data/hora com mais de 30 dias a partir de hoje.

Ao selecionar um intervalo de tempo (personalizado ou predefinido), intervalos de até 30 dias são baseados em amostras de dados com intervalos de 5 minutos. Intervalos de tempo superiores a 30 dias são baseados em amostras de dados com intervalos de uma hora.



1. Clique na caixa suspensa **Intervalo de tempo** e o painel Intervalo de tempo é exibido.
2. Para selecionar um intervalo de tempo predefinido, clique em um dos botões **Últimos…** à direita do painel **Intervalo de Tempo**. Ao selecionar um intervalo de tempo predefinido, os dados de até 13 meses ficam

disponíveis. O botão do intervalo de tempo predefinido selecionado é destacado, e os dias e horários correspondentes são exibidos nos calendários e seletores de tempo.

3. Para selecionar um intervalo de datas personalizado, clique na data inicial no calendário **De** à esquerda. Clique em **<** or **>** 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 fica destacado, indicando que você selecionou um intervalo de datas personalizado.
4. Para selecionar um intervalo de tempo personalizado, clique no controle **Hora** abaixo do calendário **De** e selecione a hora de início. Para especificar a hora de término, clique no controle **Hora** abaixo do calendário **Até** à direita e selecione a hora de término. O botão **Intervalo Personalizado** à direita do painel Intervalo de Tempo fica 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, em seguida, 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 de **Time** e o botão **Custom Range** é destacado.
6. Após selecionar o intervalo de data e hora, clique em **Aplicar intervalo**. As estatísticas de desempenho desse intervalo de tempo são exibidas nos gráficos e na linha do tempo de eventos.

Defina objetos correlacionados para gráficos de comparação no Active IQ Unified Manager

No painel Gráfico de contadores, você pode definir uma lista de objetos correlacionados para comparação de dados e desempenho. Por exemplo, se sua máquina virtual de armazenamento (SVM) estiver apresentando um problema de desempenho, você pode comparar todos os volumes da SVM para identificar qual volume pode estar causando o problema.

Você pode adicionar qualquer objeto da grade de objetos correlacionados aos painéis de gráfico de comparação e 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 de comparação não pode ser removido.

Adicionar muitos objetos ao painel Comparar pode afetar negativamente o desempenho. Para manter o desempenho, selecione 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 Comparando. Os dados do objeto são adicionados aos gráficos nos painéis Gráficos de Contador. A cor do ícone de olho do objeto ( ) corresponde à cor da linha de tendência dos dados do objeto nos gráficos.

2. **Opcional:** Ocultar ou exibir dados para objetos selecionados:

Para fazer isso…	Faça o seguinte…
Ocultar um objeto selecionado	Clique no ícone de olho ( ) do objeto selecionado no painel Comparing. Os dados do objeto ficam ocultos, e o ícone de olho desse objeto fica cinza.
Mostrar um objeto oculto	Clique no ícone de olho cinza do objeto selecionado no painel Comparing. O ícone do olho retorna à sua cor original, e os dados do objeto são adicionados novamente aos gráficos no painel Gráficos de Contador.

3. **Opcional:** Remova os objetos selecionados do painel **Comparing**:

Para fazer isso…	Faça o seguinte…
Remover um objeto selecionado	No painel Comparando, passe o cursor sobre o nome do objeto selecionado para exibir o botão Remover objeto (**X**) e clique nele. O objeto é removido do painel Comparando, e seus dados são apagados dos gráficos de contadores.
Remover todos os objetos selecionados	Clique no botão "Remover todos os objetos" (**X**) na parte superior do painel de comparação. Todos os objetos selecionados e seus dados são removidos, restando apenas o objeto raiz.

Entenda os gráficos de contadores no Active IQ Unified Manager

Os gráficos no painel Gráficos de Contador permitem que você visualize e compare dados de desempenho do objeto raiz e dos objetos que você adicionou na grade de objetos correlacionados. Isso pode ajudar você a entender as tendências de desempenho, bem como a isolar e resolver problemas de desempenho.

Os gráficos de contador exibidos por padrão são Eventos, Latência, IOPS e MBps. Os gráficos opcionais que você pode escolher exibir são Utilização, Capacidade de Desempenho Usada, IOPS Disponíveis, IOPS/TB e Taxa de Falha de Cache. Além disso, você pode optar por visualizar os valores totais ou os valores detalhados dos gráficos de Latência, IOPS, MBps e Capacidade de Desempenho Usada.

O Performance Explorer exibe determinados gráficos de contadores por padrão, independentemente de o objeto de storage oferecer suporte a todos eles ou não. Quando um contador não é suportado, o gráfico de contador fica vazio e a mensagem `Not applicable for <object>` é exibida.

Os gráficos exibem as 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 as unidades de contador exclusivas do objeto ou dos objetos selecionados.

As cores das linhas de tendência correspondem à cor do nome do objeto 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 deseja analisar um período específico em um gráfico, pode usar um dos seguintes métodos:

- Use o botão **<** para expandir o painel Counter Charts para ocupar toda a largura da página.
- Use o cursor, quando ele se transformar em uma lupa, para selecionar uma parte do período no gráfico, concentrar-se nessa área e ampliá-la. Você pode clicar em "Redefinir zoom do gráfico" para retornar o gráfico ao período padrão.
- Use o botão **Visualização Ampliada** para exibir um gráfico de contador único ampliado que contém detalhes expandidos e indicadores de limite.

Ocasionalmente, podem aparecer lacunas nas linhas de tendência. Essas lacunas significam que o Unified Manager não conseguiu coletar dados de desempenho do sistema de storage ou que o Unified Manager pode ter estado inativo.

Entenda os tipos de gráficos de contadores de desempenho no Active IQ Unified Manager

Existem gráficos de desempenho padrão que exibem os valores dos contadores para o objeto de armazenamento selecionado. Cada um dos gráficos de detalhamento de contadores exibe os valores totais separados em leitura, gravação e outras categorias. Além disso, alguns gráficos de detalhamento de contadores exibem detalhes adicionais quando o gráfico é visualizado no modo de 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 informativos em correlação com os gráficos estatísticos do objeto raiz. Os eventos de integridade são exibidos em conjunto com os eventos de desempenho para fornecer uma visão completa dos motivos pelos quais o desempenho pode ser afetado.
Latência total	Número de milissegundos necessários para responder às solicitações da aplicação. Observe que os valores médios de latência são ponderados por E/S.
Latência: detalhamento	As mesmas informações exibidas em Latency Total, mas com os dados de desempenho separados em latência de leitura, gravação e outras latências. Esta opção de gráfico aplica-se somente quando o objeto selecionado é uma SVM, nó, agregado, volume, LUN ou namespace.

Gráficos disponíveis	Descrição do gráfico
Latência: componentes do cluster	As mesmas informações exibidas em Latency 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” mostra o IOPS para dados que trafegam por esse nó, que podem residir no nó local ou remoto, e selecionar “Total (Local)” mostra o IOPS para dados que residem apenas no nó atual.
IOPS: detalhamento	As mesmas informações exibidas em IOPS Total, mas com os dados de desempenho separados em IOPS de leitura, gravação e outros. Esta opção de gráfico se aplica somente quando o objeto selecionado é uma SVM, nó, agregado, volume, LUN ou namespace. Quando exibido na visualização Zoom, o gráfico de volumes mostra os valores mínimos e máximos de throughput de QoS, se configurados no ONTAP. Ao exibir para um nó, selecionar “Detalhamento” exibe a distribuição de IOPS para os dados que trafegam por esse nó, que podem residir no nó local ou no nó remoto, e selecionar “Detalhamento (Local)” exibe a distribuição de IOPS para os dados que residem apenas no nó atual.
IOPS - Protocolos	As mesmas informações exibidas em IOPS Total, mas os dados de desempenho são separados em gráficos individuais para o tráfego de protocolo CIFS, NFS, FCP, NVMe e iSCSI. Esta opção de gráfico se aplica somente quando o objeto selecionado é uma SVM.
IOPS/TB - Total	Número de operações de entrada/saída processadas por segundo, com base no espaço total 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 storage. Quando exibido na visualização Zoom, o gráfico de volumes mostra os valores de throughput esperado e máximo de QoS, se configurados no ONTAP. Esta opção de gráfico só se aplica quando o objeto selecionado é um volume.
MB/s - total	Número de megabytes de dados transferidos de e para o objeto por segundo.

Gráficos disponíveis	Descrição do gráfico
MB/s - Detalhamento	As mesmas informações mostradas no gráfico de MB/s, mas com os dados de taxa de transferência separados em leituras de disco, leituras do Flash Cache, gravações e outros. Quando exibido na visualização Zoom, o gráfico de volumes mostra os valores máximos de taxa de transferência de QoS, se configurados no ONTAP. Esta opção de gráfico só se aplica quando o objeto selecionado é uma SVM, nó, agregado, volume, LUN ou namespace. Os dados do Flash Cache são exibidos apenas para nós e somente quando um módulo do 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	Os dados de capacidade de desempenho utilizada são separados em protocolos de usuário e processos em segundo plano do sistema. Além disso, é exibida a quantidade de capacidade de desempenho livre.
IOPS disponíveis - total	Número de operações de entrada/saída por segundo atualmente disponíveis (livres) neste objeto. Este número resulta da subtração das IOPS atualmente utilizadas do total de IOPS que o Unified Manager calcula que o objeto pode realizar. Esta opção de gráfico se aplica apenas quando o objeto selecionado é um nó ou agregado.
Utilização - Total	Percentual de recursos disponíveis do objeto que está em uso. A utilização indica a utilização do nó para nós, a utilização do disco para agregados e a utilização de largura de banda para portas. Esta opção de gráfico se aplica somente quando o objeto selecionado é um nó, agregado ou porta.
Taxa de falha de cache - Total	Porcentagem das solicitações de leitura de aplicativos cliente que são retornadas do disco em vez de serem retornadas do cache. Esta opção de gráfico se aplica apenas quando o objeto selecionado é um volume.

Selecione os gráficos de desempenho a serem exibidos no Active IQ Unified Manager

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 de Contadores**, clique na lista suspensa **Escolher gráficos**.
2. Adicionar ou remover gráficos:

Para…	Faça isso…
Adicionar ou remover gráficos individuais	Marque as caixas de seleção ao lado dos gráficos que deseja mostrar ou ocultar
Adicionar todos os gráficos	Clique em **Selecionar tudo**
Remova 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 de Contadores para corresponder à ordem dos gráficos listados na lista suspensa Escolher gráficos. Selecionar gráficos adicionais pode exigir rolagem adicional.

Expanda o painel Gráficos de Contadores no Active IQ Unified Manager

Você pode expandir o painel Gráficos do contador para que os gráficos fiquem maiores e mais legíveis.

Depois de definir os objetos de comparação e o intervalo de tempo dos contadores, você pode visualizar um painel Counter Charts maior. 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 Counter Charts para que ele se ajuste à largura da página	Clique no botão **<**
Reduza o painel Counter Charts para a metade direita da página	Clique no botão **>**

Altere o foco dos gráficos de contador para um período mais curto no Active IQ Unified Manager

Você pode usar o mouse para reduzir o intervalo de tempo e focar em um período específico no painel do gráfico de contadores ou na janela de visualização ampliada do gráfico de contadores. Isso permite visualizar uma perspectiva mais detalhada e microscópica de qualquer parte da linha do tempo dos dados de desempenho, eventos e limites.

Antes de começar

O cursor deve ter se transformado em uma lupa para indicar que essa funcionalidade está ativa.

Ao usar esse recurso, que altera a linha do tempo para exibir valores que correspondem à visualização mais detalhada, o intervalo de data e hora no seletor **Intervalo de Tempo** não

muda em relação aos valores originais do gráfico.

Passos

1. Para ampliar um período específico, clique usando a lupa e arraste o mouse para destacar a área que deseja visualizar 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.

Veja os detalhes do evento na linha do tempo de eventos do Active IQ Unified Manager

Você pode visualizar todos os eventos e seus respectivos detalhes no painel Events Timeline do Performance Explorer. Este é um método rápido e eficiente para visualizar todos os eventos de integridade e desempenho que ocorreram no objeto raiz durante um intervalo de tempo específico, o que pode ser útil na solução de problemas de desempenho.

O painel Linha do tempo de eventos exibe eventos críticos, de erro, de aviso e informativos que ocorreram no objeto raiz durante o intervalo de tempo selecionado. Cada nível de severidade de evento tem sua própria linha do tempo. Eventos únicos e múltiplos são representados por um ponto de evento na linha do tempo. Você pode posicionar o cursor sobre um ponto de evento para ver os detalhes do evento. Para aumentar a granularidade visual de múltiplos eventos, você pode diminuir o intervalo de tempo. Isso distribui múltiplos 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 contador exibidos abaixo da Linha do Tempo de Eventos. Isso proporciona uma correlação visual direta entre os eventos e o desempenho geral. Os eventos de integridade também são exibidos na linha do tempo, mas esses tipos de eventos não se alinham necessariamente com 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 na linha do tempo para visualizar um resumo do evento ou dos eventos naquele ponto do evento.

   Uma janela pop-up exibe informações sobre os tipos de eventos, a data e a hora em que os eventos ocorreram, o estado e a duração do evento.

2. Veja os detalhes completos de um ou mais eventos:

Para fazer isso…	Clique aqui…
Veja os detalhes de um único evento	**Ver detalhes do evento** na caixa de diálogo pop-up.

Para fazer isso…	Clique aqui…
Veja os detalhes de vários eventos	**Ver detalhes do evento** na caixa de diálogo pop-up. Ao clicar em um único evento na caixa de diálogo de vários eventos, você abre a página correspondente de detalhes do evento.

Visualização ampliada dos gráficos de contadores

Saiba mais sobre a visualização de zoom em Gráficos de Contadores no Active IQ Unified Manager

Os gráficos de contador oferecem uma visualização com zoom que permite ampliar os detalhes de desempenho ao longo do período especificado. Isso permite que você veja detalhes de desempenho e eventos com muito mais granularidade, o que é útil na solução de problemas de desempenho.

Quando exibidos na Zoom View, alguns dos gráficos de detalhamento fornecem informações adicionais além do que aparece quando o gráfico não está na Zoom View. Por exemplo, as páginas da Zoom View dos gráficos de detalhamento de IOPS, IOPS/TB e MBps exibem os valores da política de QoS para volumes e LUNs, caso tenham sido configurados no ONTAP.

Para políticas de limite de desempenho definidas pelo sistema, apenas as políticas “Node resources over-utilized” e “QoS throughput limit breached” estão disponíveis na lista **Policies**. As outras políticas de limite definidas pelo sistema não estão disponíveis no momento.

Exiba a visualização ampliada dos gráficos de contador no Active IQ Unified Manager

A visualização ampliada dos gráficos de contador fornece um nível de detalhe mais preciso para o gráfico de contador selecionado e sua linha do tempo associada. Isso amplia os dados do gráfico de contador, permitindo uma visão mais clara dos eventos de desempenho e suas causas subjacentes.

Você pode exibir a visualização ampliada dos gráficos de contador para qualquer gráfico de contador.

Passos

1. Clique em **Visualização Ampliada** para abrir o gráfico selecionado em uma nova janela do navegador.
2. Se você estiver visualizando um gráfico de detalhamento e clicar em **Zoom View**, o gráfico de detalhamento será exibido em **Zoom View**. Você pode selecionar **Total** enquanto estiver em **Zoom View** se quiser alterar a opção de visualização.

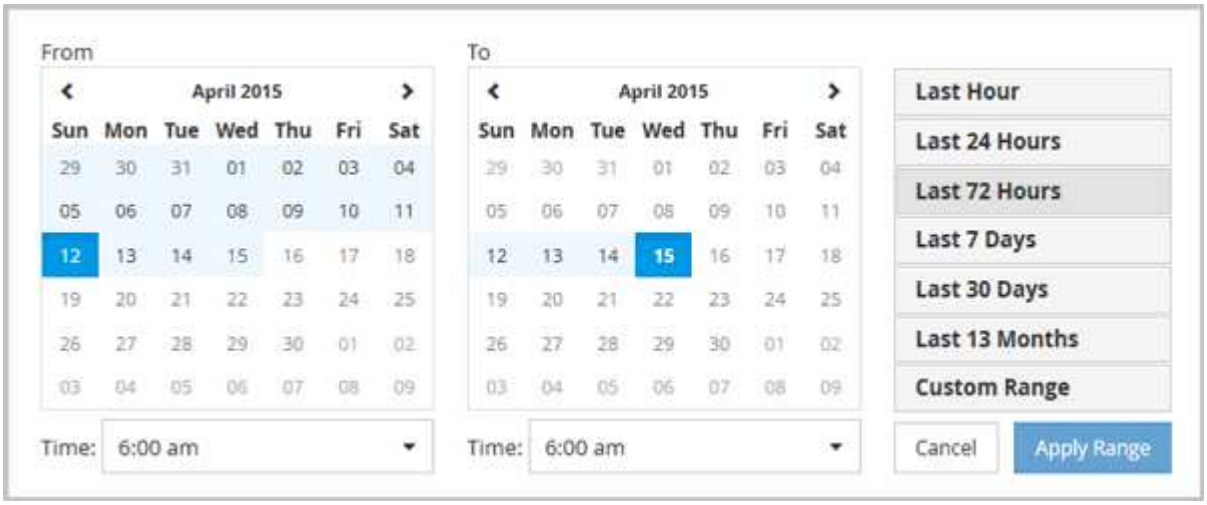
Especifique o intervalo de tempo na visualização Zoom no Active IQ Unified Manager

O controle **Intervalo de Tempo** na janela de visualização ampliada dos gráficos de contador permite especificar um intervalo de data e hora para o gráfico selecionado. Isso possibilita localizar rapidamente dados específicos com base em um intervalo de tempo predefinido ou em um intervalo de tempo personalizado.

Você pode selecionar um intervalo de tempo entre uma hora e 390 dias. Treze meses equivalem a 390 dias, pois 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 na solução de possíveis problemas de desempenho, pois especificar um intervalo de data e hora exibe com mais detalhes os dados ao redor do evento de desempenho. Use o controle **Intervalo de Tempo** para selecionar intervalos predefinidos de data e hora ou especifique seu próprio intervalo personalizado de data e hora de até 390 dias. Os botões de intervalos de tempo predefinidos variam de **Última Hora** a **Últimos 13 Meses**.

Selecionar a opção **Últimos 13 meses** ou especificar um intervalo de datas personalizado superior a 30 dias exibe uma caixa de diálogo alertando que os dados de desempenho exibidos para um período superior a 30 dias são apresentados em gráfico usando médias horárias, e não dados coletados a cada 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 será exibida quando você selecionar a opção **Últimos 13 meses** ou especificar um intervalo de datas personalizado superior a 30 dias. Os dados resumidos também se aplicam a um intervalo de tempo menor, se o intervalo de tempo incluir uma data/hora com mais de 30 dias a partir de hoje.

Ao selecionar um intervalo de tempo (personalizado ou predefinido), intervalos de até 30 dias são baseados em amostras de dados com intervalos de 5 minutos. Intervalos de tempo superiores a 30 dias são baseados em amostras de dados com intervalos de uma hora.



1. Clique na caixa suspensa **Intervalo de tempo** e o painel Intervalo de tempo é exibido.
2. Para selecionar um intervalo de tempo predefinido, clique em um dos botões **Últimos…** à direita do painel **Intervalo de Tempo**. Ao selecionar um intervalo de tempo predefinido, os dados de até 13 meses ficam disponíveis. O botão do intervalo de tempo predefinido selecionado é destacado, e os dias e horários correspondentes são exibidos nos calendários e seletores de tempo.
3. Para selecionar um intervalo de datas personalizado, clique na data inicial no calendário **De** à esquerda. Clique em **<** or **>** 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 fica destacado, indicando que você selecionou um intervalo de datas personalizado.
4. Para selecionar um intervalo de tempo personalizado, clique no controle **Hora** abaixo do calendário **De** e selecione a hora de início. Para especificar a hora de término, clique no controle **Hora** abaixo do calendário **Até** à direita e selecione a hora de término. O botão **Intervalo Personalizado** à direita do painel Intervalo de Tempo fica 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, em seguida, 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 de **Time** e o botão **Custom Range** é destacado.
6. Após selecionar o intervalo de data e hora, clique em **Aplicar intervalo**. As estatísticas de desempenho desse intervalo de tempo são exibidas nos gráficos e na linha do tempo de eventos.

Selecione os limites de desempenho na visualização ampliada dos gráficos de contador em Active IQ Unified Manager

Aplicar limites na visualização ampliada 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 imediatamente os resultados, o que pode ser útil para decidir se solucionar problemas deve ser sua próxima etapa.

A seleção de limiares na visualização ampliada dos gráficos de contadores permite visualizar dados precisos sobre eventos de limite de desempenho. Você pode aplicar qualquer limiar que apareça na área **Policies** da visualização ampliada dos gráficos de contadores.

Na visualização ampliada dos gráficos de contador, apenas uma política pode ser aplicada por vez ao objeto.

Etapa

1. Selecione ou desmarque a opção associada a uma política.

   O limite selecionado é aplicado à visualização ampliada dos gráficos de contador. Os limites críticos são exibidos como uma linha vermelha; os limites de alerta são exibidos como uma linha amarela.

Visualize a latência por componente de cluster no Active IQ Unified Manager

Você pode visualizar informações detalhadas de latência de um volume usando a página Volume Performance Explorer. O gráfico de contadores Latency - Total mostra a latência total no volume, e o gráfico de contadores Latency - Breakdown 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 clusters
- Data Processing
- Operações de agregado
- Ativação de volume
- MetroCluster Recursos

- Latência na nuvem
- Sincronizar o SnapMirror

Passos

1. Na página **Volume Performance Explorer** do volume selecionado, no gráfico **Latency**, selecione **Cluster Components** no menu suspenso.

   O gráfico Latência - Componentes do cluster é exibido.

2. Para visualizar uma versão ampliada do gráfico, selecione **Visualização com zoom**.

   O gráfico comparativo dos componentes do cluster é exibido. Você pode restringir a comparação desmarcando ou marcando o associado a cada componente do cluster.

3. Para visualizar os valores específicos, mova o seu cursor para a área do gráfico para ver a janela pop-up.

Visualize o tráfego de IOPS da SVM por protocolo no Active IQ Unified Manager

Você pode visualizar informações detalhadas de IOPS para uma SVM usando a página Performance/SVM Explorer. O gráfico do contador IOPS - Total mostra o uso total de IOPS na SVM, e o gráfico do contador IOPS - Breakdown é útil para determinar o impacto das operações de leitura, gravação e outras IOPS na SVM.

Além disso, o gráfico IOPS - Protocolos mostra uma comparação detalhada do tráfego de IOPS para cada protocolo utilizado na SVM. Os seguintes protocolos estão disponíveis:

- CIFS
- NFS
- FCP
- iSCSI
- NVMe-FC

Passos

1. Na página **Explorador de Desempenho/SVM** da SVM selecionada, no gráfico de IOPS, selecione **Protocolos** no menu suspenso.

   O gráfico IOPS - Protocols é exibido.

2. Para visualizar uma versão ampliada do gráfico, selecione **Visualização com zoom**.

   O gráfico comparativo avançado de protocolos IOPS é exibido. Você pode restringir a comparação desmarcando ou selecionando a opção associada a um protocolo.

3. Para visualizar os valores específicos, mova seu cursor para a área do gráfico em qualquer um dos gráficos para ver a janela pop-up.

Visualize os gráficos de latência de volume e de LUN para verificar a garantia de desempenho no Active IQ Unified Manager

Você pode visualizar os volumes e LUNs aos quais se inscreveu no programa

"Performance Guarantee" para verificar se a latência não excedeu o nível garantido para você.

A garantia de desempenho de latência é um valor em milissegundos por operação que não deve ser excedido. Ela se baseia em uma média horária, e não no período padrão de coleta de desempenho de cinco minutos.

Passos

1. Na visualização **Desempenho: Todos os Volumes** ou **Desempenho: Todas as LUNs**, selecione o volume ou a LUN de seu interesse.
2. Na página **Performance Explorer** do volume ou LUN selecionado, escolha **Hourly Average** no seletor **View statistics in**.

   A linha horizontal no gráfico de latência apresentará uma curva 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 cobertos pela garantia de desempenho, poderá adicioná-los para visualizar o valor de latência deles no mesmo gráfico.

Visualize o desempenho de todos os clusters SAN Array no Active IQ Unified Manager

Você pode usar a visualização Performance: all Clusters para exibir o status de desempenho dos seus clusters All SAN Array.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Você pode visualizar informações gerais de todos os clusters SAN Array na visualização Performance: All Clusters e detalhes na página Cluster / Performance Explorer.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Clusters**.
2. Certifique-se de que a coluna “Personality” esteja visível na visualização **Health: All Clusters** ou adicione-a usando o controle **Show / Hide**.

   Esta coluna exibe “All SAN Array” para seus clusters All SAN Array.

3. Para visualizar informações sobre o desempenho nesses clusters, selecione a visualização **Performance: All Clusters**.

   Veja as informações de desempenho do cluster All SAN Array.

4. Para visualizar informações detalhadas sobre o desempenho nesses clusters, clique no nome de um cluster All SAN Array.
5. Clique na guia **Explorer**.
6. Na página **Cluster / Performance Explorer**, selecione **Nodes on this Cluster** no menu **View and Compare**.

   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 mais longo para

identificar quaisquer problemas de configuração.

Visualize as IOPS do nó com base nas cargas de trabalho locais no Active IQ Unified Manager

O gráfico do contador de IOPS do nó pode destacar onde as operações estão apenas passando pelo nó local usando uma LIF de rede para executar operações de leitura/gravação em volumes em um nó remoto. Os gráficos de IOPS, “Total (Local)” e “Breakdown (Local)”, exibem os IOPS de dados que residem apenas em volumes locais no nó atual.

As versões “Local” desses gráficos de contadores são semelhantes aos gráficos de nós de capacidade de desempenho e utilização, pois também mostram apenas as estatísticas dos dados que residem em volumes locais.

Ao comparar as versões “Local” desses gráficos de contador com as versões regulares “Total” desses gráficos de contador, 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 por alta utilização no nó, caso haja muitas operações passando pelo nó local para alcançar um volume em um nó remoto. Nesses casos, talvez você queira mover um volume para o nó local ou criar uma LIF no nó remoto à qual o tráfego dos hosts que acessam esse volume possa se conectar.

Passos

1. Na página **Performance/Node Explorer** do nó selecionado, no gráfico de IOPS, selecione **Total** no menu suspenso.

   O gráfico IOPS - Total é exibido.

2. Clique em **Visualização ampliada** para exibir uma versão maior do gráfico em uma nova aba do navegador.
3. De volta à página **Performance/Node Explorer**, no gráfico de IOPS, selecione **Total (Local)** no menu suspenso.

   O gráfico IOPS - Total (Local) é exibido.

4. Clique em **Visualização ampliada** para exibir uma versão maior do gráfico em uma nova aba do navegador.
5. Visualize os dois gráficos lado a lado e identifique as áreas em que os valores de IOPS parecem ser bastante diferentes.
6. Mova o cursor sobre essas áreas para comparar o IOPS local e total em um ponto específico no tempo.

Componentes das páginas de destino do objeto

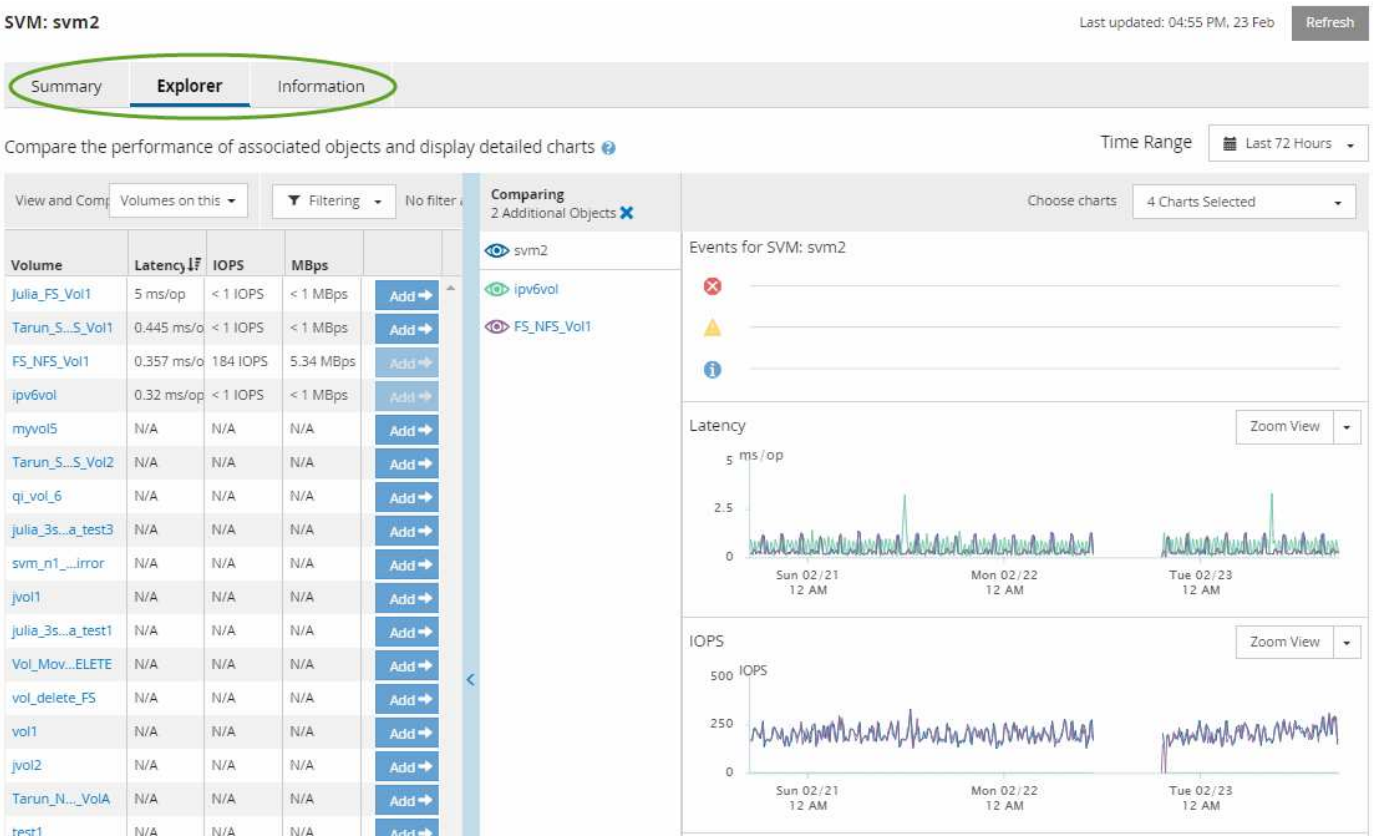
Analise os componentes das páginas de destino de objetos no Active IQ Unified Manager

As páginas de destino dos objetos fornecem detalhes sobre todos os eventos críticos, de aviso e informativos. Elas oferecem uma visão detalhada do desempenho de todos os objetos do cluster, permitindo que você selecione e compare objetos individuais em diferentes períodos.

As páginas de destino de objetos permitem examinar o desempenho geral de todos os objetos e comparar os dados de desempenho de cada objeto lado a lado. Isso é útil para avaliar o desempenho e solucionar problemas.

> 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 inicial de objeto exibindo as informações do Explorer:



Dependendo do objeto de armazenamento que está sendo visualizado, a página inicial do objeto pode conter 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 durante o período anterior de 72 horas, incluindo uma linha de tendência que mostra os valores máximo e mínimo durante esse período.

- Explorador

  Exibe uma grade de objetos de armazenamento relacionados ao objeto atual, permitindo comparar os valores de desempenho do objeto atual com os dos objetos relacionados. Esta guia inclui até onze gráficos de contador e um seletor de intervalo de tempo, possibilitando diversas comparações.

- Informação

  Exibe os valores dos atributos de configuração não relacionados ao desempenho do objeto de

armazenamento, incluindo a versão instalada do software ONTAP, o nome do parceiro de alta disponibilidade (HA) e o número de portas e LIFs.

- Melhores desempenhos

  Para clusters: exibe os objetos de armazenamento com o melhor ou o pior desempenho, com base no contador de desempenho selecionado.

- Planejamento de failover

  Para nós: exibe a estimativa do impacto no desempenho de um nó caso o parceiro de alta disponibilidade (HA) do nó falhe.

- Detalhes

  Para volumes: exibe estatísticas detalhadas de desempenho para todas as atividades e operações de E/S da carga de trabalho do volume selecionado. Esta guia está disponível para volumes FlexVol, volumes FlexGroup e componentes de FlexGroups.

Analise a página de Resumo de Desempenho em Active IQ Unified Manager

A página Resumo exibe gráficos de contadores que contêm detalhes sobre os eventos e o desempenho por objeto nas 72 horas anteriores. Esses dados não são atualizados automaticamente, mas estão atuais até o último carregamento da página. Os gráficos na página Resumo respondem à pergunta *Preciso verificar mais alguma coisa?*

Gráficos e estatísticas de contador

Os gráficos de resumo fornecem uma visão geral rápida e de alto nível das últimas 72 horas e ajudam você a identificar possíveis problemas que exigem investigação mais aprofundada.

As estatísticas de contadores da página Summary são exibidas em gráficos.

Você pode posicionar o cursor sobre a linha de tendência em um gráfico para visualizar os valores do contador em um determinado momento. Os gráficos de resumo também exibem o número total de eventos críticos e de alerta ativos nas últimas 72 horas para os seguintes contadores:

- **Latência**

  Tempo de resposta médio para todas as solicitações de E/S; expresso em milissegundos por operação.

  Exibido para todos os tipos de objeto.

- **IOPS**

  Velocidade operacional média; expressa em operações de entrada/saída por segundo.

  Exibido para todos os tipos de objeto.

- **MB/s**

  Taxa de transferência média; expressa em megabytes por segundo.

  Exibido para todos os tipos de objeto.

- **Capacidade de desempenho utilizada**

  Porcentagem da capacidade de desempenho que está sendo consumida por um nó ou agregado.

  Exibido apenas para nós e agregados.

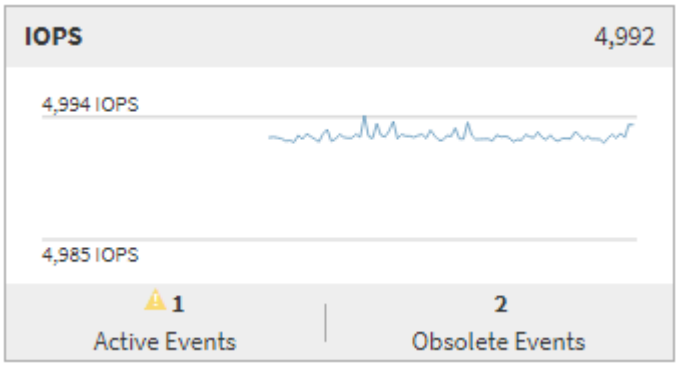
- **Utilização**

  Porcentagem de utilização de objetos para nós e agregados, ou utilização de largura de banda para portas.

  Exibido apenas para nós, agregados e portas.

Ao posicionar o cursor sobre a contagem de eventos ativos, o tipo e o número de eventos são exibidos. 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 representa o valor médio das últimas 72 horas. Os números exibidos na parte inferior e superior do gráfico de linha de tendência representam os valores mínimo e máximo das últimas 72 horas. A barra cinza abaixo do gráfico contém a contagem de eventos ativos (novos e confirmados) e eventos obsoletos das últimas 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 de 72 horas anterior. A latência refere-se ao tempo médio de resposta para todas as solicitações de E/S, expresso em milissegundos por operação, ao tempo de serviço, ao tempo de espera ou a ambos experimentados por um pacote de dados ou bloco no componente de storage do cluster em questão.

  Valor máximo (valor do contador): o número no cabeçalho exibe a média do período anterior de 72 horas.

  Gráfico do meio (desempenho): o número na parte inferior do gráfico exibe a menor latência, e o número na parte superior do gráfico exibe a maior latência para o período anterior de 72 horas. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor da latência em um horário específico.

  Parte inferior (eventos): ao passar o cursor sobre o elemento, uma janela pop-up exibe os detalhes dos eventos. Clique no link **Eventos Ativos** abaixo do gráfico para navegar até a página de Inventário de Eventos e visualizar os detalhes completos dos eventos.

- **Gráfico do contador de IOPS**

  O gráfico do contador de IOPS fornece uma visão geral de alto nível da integridade de IOPS do objeto nas 72 horas anteriores. O IOPS indica a velocidade do sistema de storage em número de operações de entrada/saída por segundo.

Valor máximo (valor do contador): o número no cabeçalho exibe a média do período anterior de 72 horas.

Gráfico do meio (desempenho): o número na parte inferior do gráfico exibe o menor valor de IOPS, e o número na parte superior do gráfico exibe o maior valor de IOPS para o período anterior de 72 horas. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor de IOPS para um horário específico.

Parte inferior (eventos): ao passar o cursor sobre o elemento, uma janela pop-up exibe os detalhes dos eventos. Clique no link **Eventos Ativos** abaixo do gráfico para navegar até a página de Inventário de Eventos e visualizar os detalhes completos dos eventos.

- **Gráfico de contador de MB/s**

  O gráfico do contador de MB/s exibe o desempenho em MB/s do objeto e indica a quantidade de dados transferidos de e para o objeto em megabytes por segundo. O gráfico do contador de MB/s fornece uma visão geral de alto nível da integridade em MB/s do objeto para o período anterior de 72 horas.

  Valor máximo (contador): o número no cabeçalho exibe a média de MB/s no período anterior de 72 horas.

  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 para o período anterior de 72 horas. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor de MB/s em um horário específico.

  Parte inferior (eventos): ao passar o cursor sobre o elemento, uma janela pop-up exibe os detalhes dos eventos. Clique no link **Eventos Ativos** abaixo do gráfico para navegar até a página de Inventário de Eventos e visualizar os detalhes completos dos eventos.

- **Gráfico do contador Capacidade de desempenho usada**

  O gráfico do contador Capacidade de Desempenho Utilizada exibe a porcentagem da capacidade de desempenho consumida pelo objeto.

  Valor máximo (contador): o número no cabeçalho exibe a capacidade média de desempenho utilizada nas últimas 72 horas.

  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 anterior de 72 horas. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor da capacidade de desempenho utilizada em um horário específico.

  Parte inferior (eventos): ao passar o cursor sobre o elemento, uma janela pop-up exibe os detalhes dos eventos. Clique no link **Eventos Ativos** abaixo do gráfico para navegar até a página de Inventário de Eventos e visualizar os detalhes completos dos eventos.

- **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 utilização de largura de banda no período anterior de 72 horas.

  Valor superior (valor do contador): o número no cabeçalho exibe a porcentagem média de utilização no

período anterior de 72 horas.

Gráfico do meio (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 no período anterior de 72 horas. Posicione o cursor sobre a linha de tendência do gráfico para visualizar o valor de utilização em um horário específico.

Parte inferior (eventos): ao passar o cursor sobre o elemento, uma janela pop-up exibe os detalhes dos eventos. Clique no link **Eventos Ativos** abaixo do gráfico para navegar até a página de Inventário de Eventos e visualizar os detalhes completos dos eventos.

Eventos

A tabela de histórico de eventos, quando aplicável, lista os eventos mais recentes que ocorreram nesse objeto. Clicar no nome do evento exibe os detalhes do evento na página Event Details.

Analise a página Performance Explorer no Active IQ Unified Manager

A página do Performance Explorer permite comparar o desempenho de objetos semelhantes em um cluster, por exemplo, todos os volumes em um cluster. Isso é útil para solucionar problemas de desempenho e ajustar o desempenho dos objetos. Você também pode comparar objetos com o objeto raiz, que é a linha de base em relação à qual as comparações com outros 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 obter informações importantes sobre as definições de configuração de storage deste objeto, o que pode ajudar na solução de problemas.

A página Performance Explorer exibe uma lista de objetos do cluster e seus dados de desempenho. Esta página exibe todos os objetos do cluster do mesmo tipo (por exemplo, volumes e suas estatísticas de desempenho específicas do objeto) em formato tabular. Essa visualização fornece uma visão geral eficiente do desempenho dos objetos do cluster.

Se “N/A” aparecer em alguma célula da tabela, significa que não há valor disponível para esse contador porque não há operações de E/S nesse objeto no momento.

A página do Performance Explorer contém os seguintes componentes:

- **Período 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 será exibido na grade.

  As opções disponíveis dependem do tipo de objeto raiz e dos dados disponíveis. Você pode clicar na lista suspensa "View and Compare" para selecionar um tipo de objeto. O tipo de objeto que você seleciona é exibido na lista.

- **Filtragem**

Permite restringir a quantidade de dados que você recebe, 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 de comparação são exibidos nos gráficos de contadores.

- **Ver estatísticas em**

  Para volumes e LUNs, permite selecionar se as estatísticas são exibidas após cada ciclo de coleta (padrão de 5 minutos) ou se as estatísticas são mostradas como uma média horária. Essa funcionalidade permite visualizar o gráfico de latência em suporte ao programa "Performance Guarantee" da NetApp.

- **Gráficos de contadores**

  Exibe dados em gráfico para cada categoria de desempenho do objeto.

  Normalmente, apenas três ou quatro gráficos são exibidos por padrão. O componente "Choose charts" permite exibir gráficos adicionais ou ocultar gráficos específicos. Você também pode optar por mostrar ou ocultar a "Events Timeline".

- **Cronologia dos Eventos**

  Exibe eventos de desempenho e integridade que ocorrem ao longo da linha do tempo selecionada no componente Time Range.

Gerencie o desempenho usando informações do grupo de políticas de QoS

Gerencie o desempenho usando informações do grupo de políticas de QoS no Active IQ Unified Manager

O Unified Manager permite que você visualize os grupos de políticas de qualidade do serviço (QoS) disponíveis em todos os clusters que você está monitorando. As políticas podem ter sido definidas usando o software ONTAP (o System Manager ou o ONTAP CLI) ou pelas políticas de Performance Service Level do Unified Manager. O Unified Manager também exibe quais volumes e LUNs têm um grupo de políticas de QoS atribuído.

Para obter mais informações sobre como ajustar as configurações de QoS, consulte "Visão geral do gerenciamento de desempenho"

Controle a taxa de transferência da carga de trabalho com QoS de storage no Active IQ Unified Manager

Você pode criar um grupo de políticas de qualidade do 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 pode 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 todo o limite de taxa de transferência. 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 os IOPS combinados para que não excedessem 9.000 IOPS.

Os grupos de políticas de QoS “adaptável” também podem ser atribuídos a cargas de trabalho individuais ou a múltiplas cargas de trabalho. No entanto, mesmo quando atribuídos a múltiplas cargas de trabalho, cada carga de trabalho recebe o limite total de taxa de transferência, em vez de compartilhar o valor da taxa de transferência com outras cargas de trabalho. Além disso, as políticas de QoS adaptativas ajustam automaticamente a configuração de taxa de transferência com base no tamanho do volume, por carga de trabalho, mantendo assim a proporção de IOPS por terabyte à medida que o tamanho do volume muda. Por exemplo, se o pico for definido como 5.000 IOPS/TB em uma política de QoS adaptativa, um volume de 10 TB terá uma taxa de transferência máxima de 50.000 IOPS. Se o volume for redimensionado posteriormente para 20 TB, a QoS adaptativa 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 usam tamanhos de bloco muito grandes e, consequentemente, uma grande porcentagem da taxa de transferência.

Para políticas de QoS de grupo compartilhadas, 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 visualização Performance: All Volumes, você pode classificar os volumes afetados por IOPS e MB/s para ver quais cargas de trabalho têm o maior uso e podem 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 IOPS ou a taxa de transferência em MBps da carga de trabalho afetada.

Ao atribuir as cargas de trabalho que estão sobrecarregando os recursos do nó a uma configuração de grupo de políticas mais restritiva, o grupo de políticas limita a atividade dessas cargas de trabalho, o que pode reduzir o uso de recursos nesse nó. No entanto, se você quiser que a carga de trabalho possa usar mais recursos do nó, poderá aumentar o valor do grupo de políticas.

Você pode usar o System Manager, os comandos do ONTAP ou o Unified Manager Performance Service Levels 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
- Transferir 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

Visualize os grupos de políticas de QoS disponíveis em todos os clusters no Active IQ Unified Manager

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 pelas políticas de Performance Service Level do Unified Manager.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Grupos de Políticas de QoS**.

   A visualização Desempenho: grupos de políticas de QoS tradicionais é exibida por padrão.

2. Veja as configurações detalhadas de cada grupo de políticas de QoS tradicional disponível.
3. Clique no botão de expansão ( ) ao lado do nome do grupo de políticas de QoS para visualizar 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 adaptável ou para visualizar todos os grupos de políticas de QoS que foram criados usando os Unified Manager Performance Service Levels.

Visualize volumes ou LUNs dentro do mesmo grupo de política de QoS no Active IQ Unified Manager

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 sobrecarregando a taxa de transferência definida para o grupo de políticas. Também pode ajudar você a decidir se é possível adicionar outros volumes ao grupo de políticas sem afetar negativamente os demais volumes.

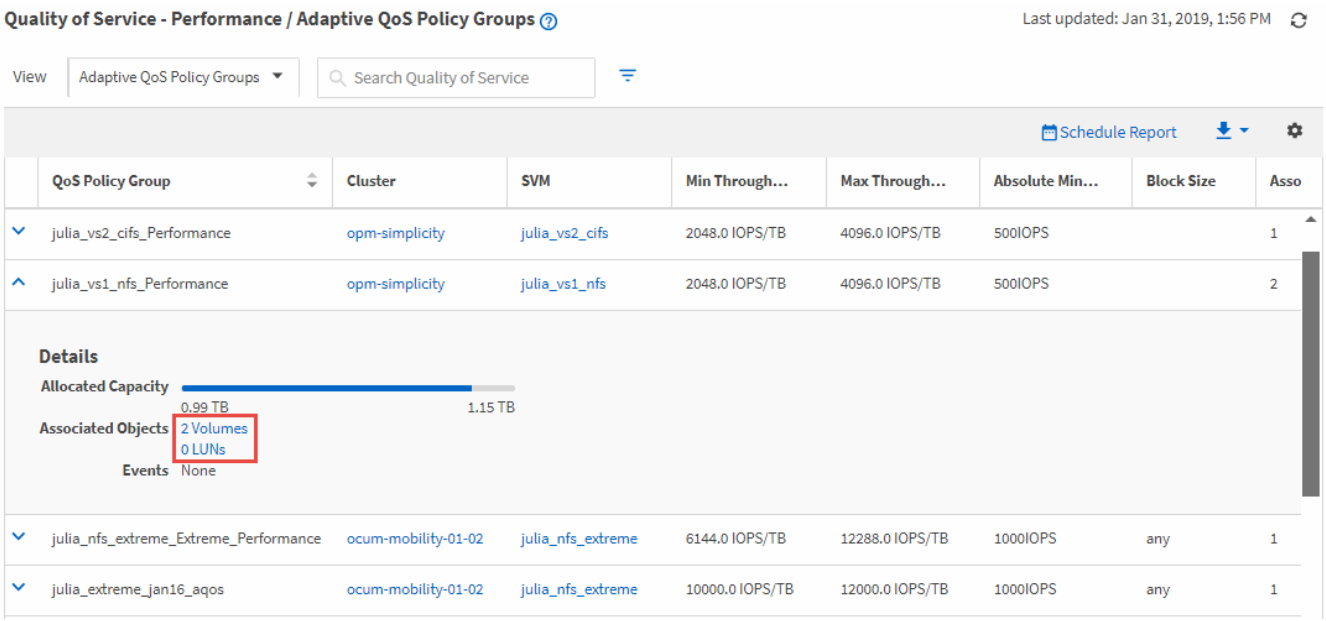
No caso de políticas de QoS adaptável e de políticas de Níveis de Serviço de Desempenho do Unified Manager, pode ser útil visualizar todos os volumes ou LUNs que estão usando um grupo de políticas para que você possa ver quais objetos seriam afetados se alterasse as configurações da política de QoS.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Grupos de Políticas de QoS**.

   A visualização Desempenho: grupos de políticas de QoS tradicionais é exibida por padrão.

2. Se você tem interesse no grupo de política tradicional, permaneça nesta página. Caso contrário, selecione uma das opções adicionais de visualização para exibir todos os grupos de políticas de QoS adaptável ou todos os grupos de políticas de QoS criados pelos Unified Manager Performance Service Levels.
3. Na política de QoS que interessa a você, clique no botão de expansão ( ) ao lado do nome do grupo de políticas de QoS para ver mais
   detalhes.



4. Clique no link Volumes ou LUNs para visualizar os objetos que utilizam esta política de QoS.

   A página de inventário de desempenho para volumes ou LUNs exibe a lista classificada de objetos que estão usando a política de QoS.

Visualize as configurações do grupo de políticas de QoS para volumes ou LUNs no Active IQ Unified Manager

Você pode ver os grupos de políticas de QoS aplicados aos seus volumes e LUNs, e pode acessar a exibição "Performance/QoS Policy Groups" para mostrar as definições de configuração detalhadas de cada política de QoS.

Os passos para visualizar a política de QoS aplicada a um volume são mostrados abaixo. Os passos para visualizar esta informação para um LUN são semelhantes.

Passos

1. No painel de navegação à esquerda, 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 analisar e role para a direita até encontrar a coluna **Grupo de Políticas de QoS**.
4. Clique no nome do QoS Policy Group.

   A página correspondente de qualidade do serviço é exibida dependendo de ser uma política de QoS tradicional, uma política de QoS adaptável ou uma política de QoS criada usando os Unified Manager Performance Service Levels.

5. Veja as configurações detalhadas do grupo de políticas de QoS.
6. Clique no botão de expansão ( ) ao lado do nome do grupo de políticas de QoS para visualizar mais detalhes sobre o grupo de políticas.

Compare volumes ou LUNs dentro do mesmo grupo de políticas de QoS no Active IQ Unified Manager

Você pode visualizar os volumes e LUNs que estão nos mesmos grupos de política de QoS e, em seguida, comparar o desempenho em um único gráfico de IOPS, MB/s ou IOPS/TB para identificar quaisquer problemas.

As etapas para comparar o desempenho de volumes no mesmo grupo de políticas de QoS são mostradas abaixo. As etapas para visualizar essas informações para um LUN são semelhantes.

Passos

1. No painel de navegação à esquerda, 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 consultar.

   A página do Explorador de Desempenho é exibida para o volume.

4. No menu Exibir e Comparar, selecione **Volumes no mesmo grupo de políticas de QoS**.

   Os demais 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 de todos os volumes selecionados nos gráficos.

   Você pode alterar o intervalo de tempo para visualizar o desempenho em diferentes períodos, além do padrão de 72 horas.

Visualize as políticas de QoS em gráficos de throughput com o Active IQ Unified Manager

Você pode visualizar as configurações de política de qualidade do serviço (QoS) definidas pelo ONTAP que foram aplicadas a um volume ou LUN no Performance Explorer e nos gráficos de IOPS, IOPS/TB e MB/s do Workload Analysis. As informações exibidas nos gráficos variam dependendo do tipo de política de QoS aplicada à carga de trabalho.

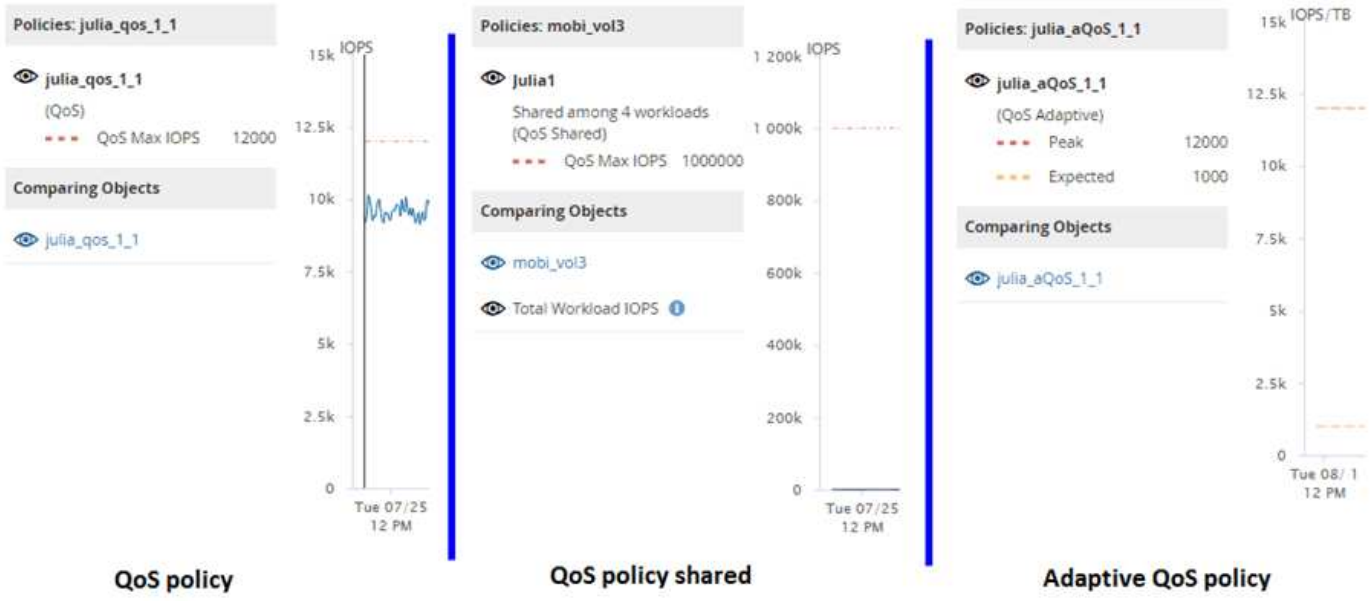
A configuração de taxa de transferência máxima (ou “pico”) define a taxa de transferência máxima que a carga de trabalho pode consumir, limitando assim o impacto sobre outras cargas de trabalho que competem por recursos do sistema. A configuração de taxa de transferência mínima (ou “esperada”) define a taxa de transferência mínima que deve estar disponível para a carga de trabalho, de modo que uma carga de trabalho crítica atenda às metas mínimas de taxa de transferência, independentemente da demanda de outras cargas de trabalho.

As políticas de QoS compartilhadas e não compartilhadas para IOPS e MB/s usam os termos “minimum” e “maximum” para definir o limite inferior e o limite superior. As políticas de QoS adaptáveis para IOPS/TB, introduzidas no ONTAP 9.3, usam os termos “expected” e “peak” para definir o limite inferior e o limite superior.

Embora o ONTAP permita criar esses dois tipos de políticas de QoS, dependendo de como elas são aplicadas às cargas de trabalho, existem 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 de QoS compartilhada atribuída a uma única carga de trabalho ou política de QoS não compartilhada 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 de QoS compartilhada atribuída a várias cargas de trabalho	Todas as cargas de trabalho compartilham a configuração de taxa de transferência especificada	Exibe “(QoS Shared)”
Política de QoS adaptável atribuída a uma única carga de trabalho ou a múltiplas 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 apresentadas nos gráficos de contador.



Quando uma política de QoS normal, definida em IOPS, aparece no gráfico IOPS/TB de uma carga de trabalho, o ONTAP converte o valor de IOPS para um valor de IOPS/TB, e o Unified Manager exibe essa política no gráfico IOPS/TB juntamente com o texto “QoS, definida em IOPS”.

Quando uma política de QoS adaptável definida em IOPS/TB aparece no gráfico de IOPS de 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 Adaptive - Used, defined in IOPS/TB” ou “QoS Adaptive - Allocated, defined in IOPS/TB”, dependendo de como a configuração de alocação de IOPS de pico está definida. Quando a configuração de alocação está definida como “allocated-space”, o IOPS de pico é calculado com base no tamanho do volume. Quando a configuração de alocação está definida como “used-space”, o IOPS de pico é calculado com base na quantidade de dados armazenados no volume, levando em consideração as eficiências de storage.

O gráfico IOPS/TB exibe dados de desempenho somente quando a capacidade lógica utilizada pelo volume é igual ou superior a 128 GB. 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 Active IQ Unified Manager

Você pode visualizar as configurações de política de qualidade do serviço (QoS) definidas pelo 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 de taxa de transferência mínima garante que uma carga de trabalho crítica atenda às metas mínimas de taxa de transferência, independentemente da demanda de cargas de trabalho concorrentes.

As configurações de throughput de QoS “minimum” e “maximum” de IOPS e MB/s são exibidas nos gráficos de contador somente se tiverem sido configuradas no ONTAP. As configurações mínimas de throughput estão disponíveis apenas em sistemas que executam o software ONTAP 9.2 ou posterior, somente em sistemas AFF, e podem ser definidas apenas para IOPS neste momento.

As políticas de QoS adaptável estão disponíveis a partir do ONTAP 9.3 e são expressas em 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 à medida que o tamanho do volume muda. Você pode aplicar um grupo de políticas de QoS adaptável somente a volumes. A terminologia de QoS “expected” e “peak” é usada para políticas de QoS adaptável em vez de mínimo e máximo.

O Unified Manager gera eventos de aviso para violações da política de QoS quando a taxa de transferência da carga de trabalho excede a configuração máxima definida da política de QoS 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 durante cada período de coleta, mas o Unified Manager exibe a taxa de transferência "média" durante o período de coleta no gráfico. Por esse motivo, você pode ver eventos de QoS enquanto a taxa de transferência de uma carga de trabalho pode não ter ultrapassado o limite da política mostrado no gráfico.

Passos

1. Na página **Explorador de Desempenho** do volume ou LUN selecionado, execute as seguintes ações para visualizar as configurações de limite máximo e mínimo de QoS:

Se você quiser…	Faça isso…
Veja o teto de IOPS (o máximo de QoS)	No gráfico IOPS Total ou de detalhamento, clique em **Visualização ampliada**.
Veja o teto de MB/s (o máximo de QoS)	No gráfico MB/s Total ou Breakdown, clique em **Zoom View**.
Veja o limite inferior de IOPS (o mínimo de QoS)	No gráfico IOPS Total ou de detalhamento, clique em **Visualização ampliada**.
Veja o teto de IOPS/TB (o pico de QoS)	Para volumes, no gráfico IOPS/TB, clique em **Visualização ampliada**.

Se você quiser…	Faça isso…
Veja o mínimo de IOPS/TB (a QoS esperada)	Para volumes, no gráfico IOPS/TB, clique em **Visualização ampliada**.

A linha horizontal tracejada indica o valor máximo ou mínimo de throughput definido no ONTAP. Você também pode visualizar 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 exibir a janela pop-up.

Se você notar que determinados volumes ou LUNs apresentam IOPS ou MB/s muito altos e estão sobrecarregando os recursos do sistema, você pode usar o System Manager ou a ONTAP CLI para ajustar as configurações de QoS, de modo 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 do gerenciamento de desempenho"

Gerencie o desempenho usando informações sobre capacidade de desempenho e IOPS disponíveis

Gerencie a capacidade de desempenho e os IOPS disponíveis no Active IQ Unified Manager

A *capacidade de desempenho* indica a quantidade de throughput que você pode obter de um recurso sem ultrapassar o desempenho útil desse recurso. Quando analisada usando os 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. A *capacidade de desempenho utilizada* é a porcentagem da capacidade de desempenho que está sendo usada no momento, e a *capacidade de desempenho livre* é a porcentagem da capacidade de desempenho que ainda está disponível.

Embora a capacidade de desempenho livre forneça uma porcentagem do recurso que ainda está disponível, o *IOPS disponível* indica 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 poderá adicionar cargas de trabalho com um número predeterminado de IOPS a um recurso.

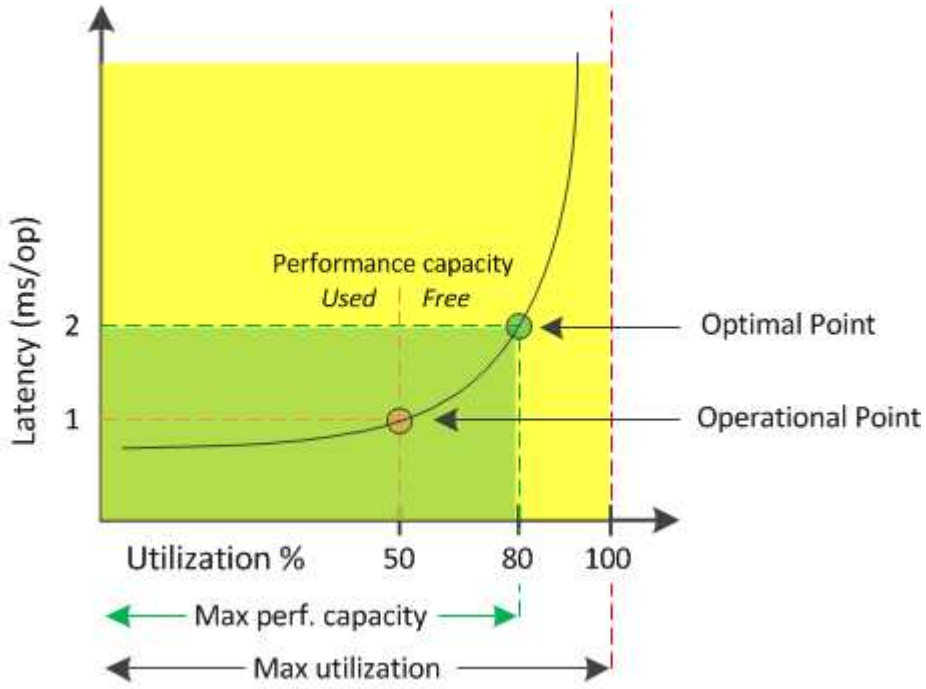
Monitorar as informações de capacidade de desempenho traz os seguintes benefícios:

- Auxilia no provisionamento e balanceamento do fluxo de trabalho.
- Ajuda você a evitar a sobrecarga de um nó ou levar seus recursos além do ponto ideal, reduzindo assim a necessidade de solucionar problemas.
- Ajuda você a determinar com maior precisão onde equipamentos de armazenamento adicionais podem ser necessários.

Entenda o contador de capacidade de desempenho usada no Active IQ Unified Manager

O contador de capacidade de desempenho utilizada ajuda a identificar se o desempenho de um nó ou agregado está atingindo um ponto em que pode se degradar com o aumento da carga de trabalho. Ele também pode mostrar se um nó ou agregado está sendo sobrecarregado durante períodos específicos. A capacidade de desempenho utilizada é semelhante à utilização, mas fornece informações mais detalhadas sobre a capacidade de desempenho disponível em um recurso físico para uma carga de trabalho específica.

A capacidade de desempenho utilizada ideal é o ponto em que um nó ou um agregado tem utilização e latência (tempo de resposta) ideais e é usado de forma eficiente. Um exemplo de curva de latência versus utilização é mostrado para um agregado na figura a seguir.



Neste exemplo, o *ponto operacional* identifica que o agregado está atualmente operando com 50% de utilização e latência de 1.0 ms/op. Com base nas estatísticas coletadas do agregado, o Unified Manager determina que há capacidade de desempenho adicional disponível para este agregado. Neste exemplo, o *ponto ideal* é identificado como o ponto em que o agregado está com 80% de utilização e latência de 2.0 ms/op. Portanto, você pode adicionar mais volumes e LUNs a este agregado para usar seus sistemas com mais eficiência.

Espera-se que o contador de capacidade de desempenho utilizada seja um número maior que o contador “utilization”, pois a capacidade de desempenho inclui o impacto na latência. Por exemplo, se um nó ou agregado estiver com 70% de utilização, o valor da capacidade de desempenho pode estar na faixa de 80% a 100%, dependendo do valor da latência.

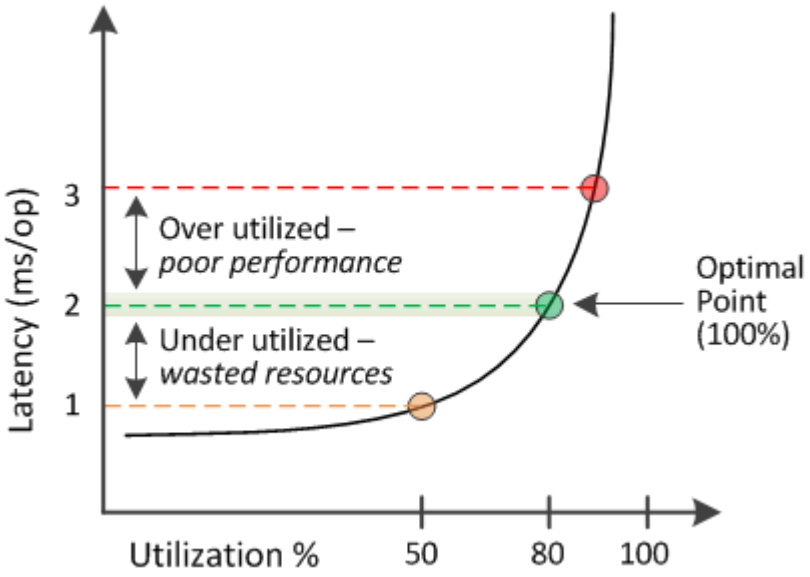
Em alguns casos, porém, o contador de utilização pode apresentar um valor maior na página Dashboard. Isso é normal, pois o dashboard atualiza os valores atuais do contador a cada período de coleta; ele não exibe médias ao longo de um período, como as outras páginas da interface de usuário do Unified Manager. O contador de capacidade de desempenho utilizada é mais adequado para indicar o desempenho médio ao longo de um período, enquanto o contador de utilização é mais indicado para determinar o uso instantâneo de

um recurso.

Utilize o valor de capacidade de desempenho usado no Active IQ Unified Manager

O valor da capacidade de desempenho utilizada ajuda você a identificar os nós e agregados que estão atualmente sobrecarregados ou subutilizados. Isso permite redistribuir as cargas de trabalho para tornar os recursos de storage 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 taxa de utilização da capacidade de desempenho igual a 100 representa o ponto ideal.

  Os recursos estão sendo usados com eficiência neste momento.

- Uma porcentagem da capacidade de desempenho usada acima de 100 indica que o nó ou agregado está sobreutilizado e que as cargas de trabalho estão recebendo desempenho abaixo do ideal.

  Não adicione novas cargas de trabalho ao recurso, e talvez seja necessário redistribuir as cargas de trabalho existentes.

- Uma porcentagem de capacidade de desempenho utilizada inferior a 100% indica que o nó ou agregado está subutilizado e que os recursos não estão sendo usados de forma eficaz.

  É possível adicionar mais cargas de trabalho ao recurso.

> Ao contrário da utilização, a porcentagem de capacidade de desempenho usada pode ultrapassar 100%. Não há um percentual máximo, mas os recursos normalmente estarão na faixa de 110% a 140% quando estiverem superutilizados. Percentuais mais altos indicariam um recurso com problemas sérios.

Entenda as IOPS disponíveis no Active IQ Unified Manager

O contador de IOPS disponíveis identifica o número restante de IOPS que podem ser adicionadas a um nó ou agregado antes que o recurso atinja seu limite.

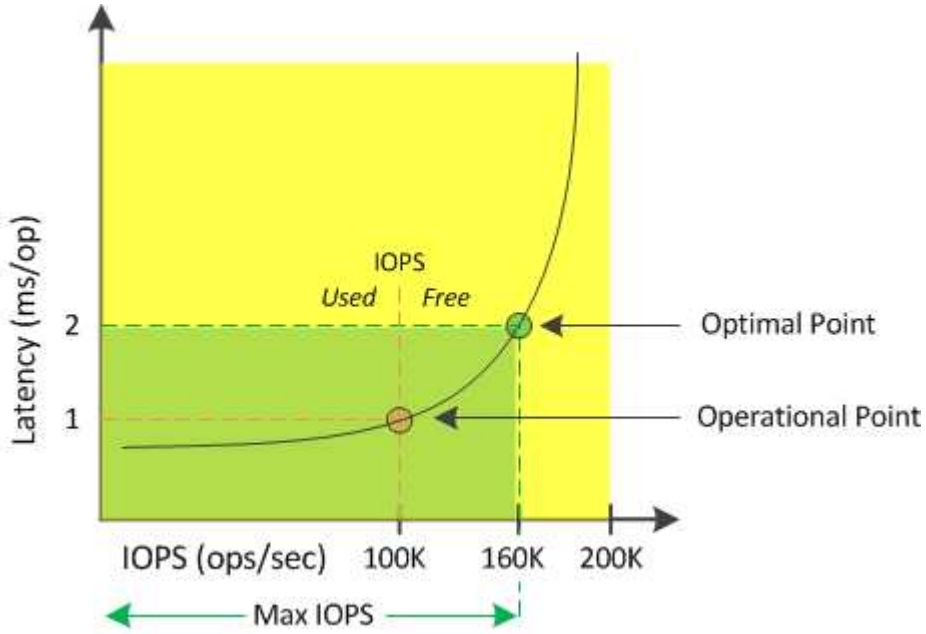
O total de IOPS que um nó pode fornecer se baseia nas características físicas do nó, por exemplo, o número de CPUs, a velocidade da CPU e a quantidade de RAM. O total de IOPS que um agregado pode fornecer se baseia nas propriedades físicas dos discos, por exemplo, um disco SATA, SAS ou SSD.

O total de IOPS de todos os volumes em um agregado pode não corresponder ao total de IOPS do agregado. Isso é discutido no seguinte artigo da base de conhecimento: KB "Por que a soma de todos os IOPs de volume em um agregado não corresponde aos IOPs do agregado?"

Enquanto o contador de capacidade de desempenho livre fornece a porcentagem 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.

A figura a seguir mostra um exemplo de curva de latência versus IOPS de um nó.



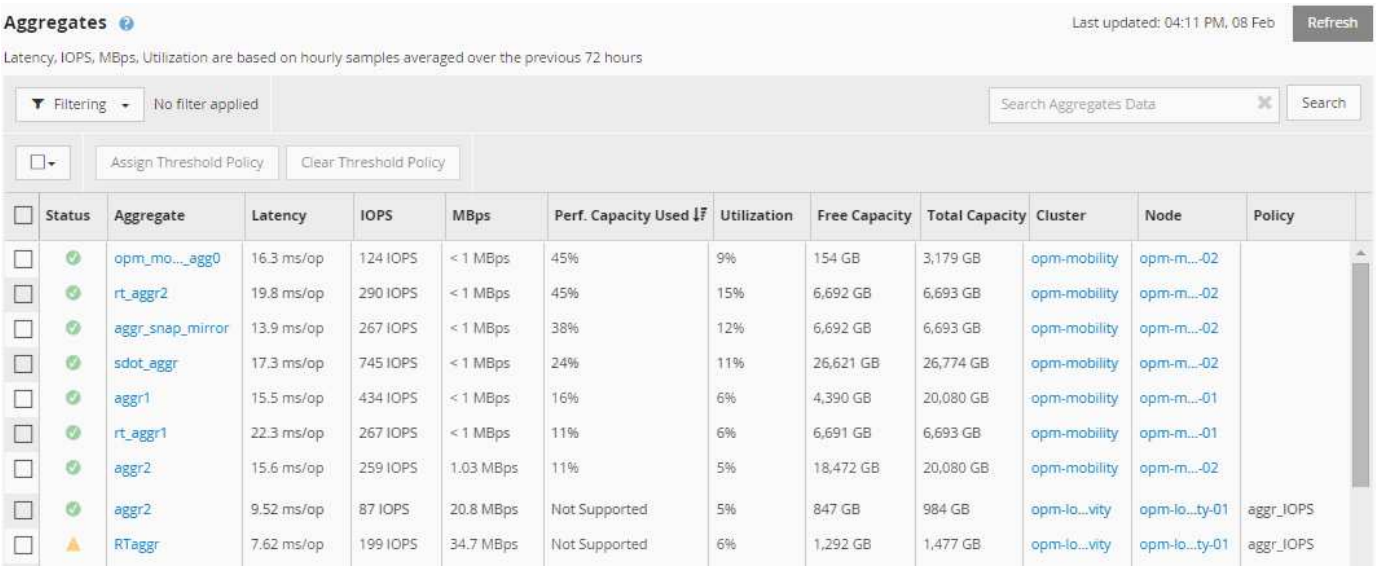
O número máximo de IOPS que um recurso pode fornecer é o número de IOPS quando o contador de capacidade de desempenho usada está em 100% (o ponto ideal). O ponto operacional indica que o nó está operando no momento a 100 mil IOPS com latência de 1,0 ms/op. Com base nas estatísticas capturadas do nó, o Unified Manager determina que o máximo de IOPS para o nó é 160 mil, o que significa que há 60 mil IOPS livres ou disponíveis. Portanto, você pode adicionar mais workloads a este nó para que seus sistemas sejam usados com mais eficiência.

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 os dados necessários para estimar com precisão as características da carga de trabalho atendida.

Visualize os valores de capacidade de desempenho de nós e agregados utilizados no Active IQ Unified Manager

Você pode monitorar os valores de capacidade de desempenho utilizados para todos os nós ou para todos os agregados em um cluster, ou pode visualizar detalhes para um único nó ou agregado.

Os valores de capacidade de desempenho utilizada aparecem no Dashboard, nas páginas Performance Inventory, na página Top Performers, na página Create Threshold Policy, nas páginas Performance Explorer e em gráficos de detalhes. Por exemplo, a página Performance: All Aggregates fornece uma coluna Performance Capacity Used para visualizar o valor de capacidade de desempenho utilizada de todos os agregados.



Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS
	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS

O monitoramento do contador de capacidade de desempenho utilizada permite identificar o seguinte:

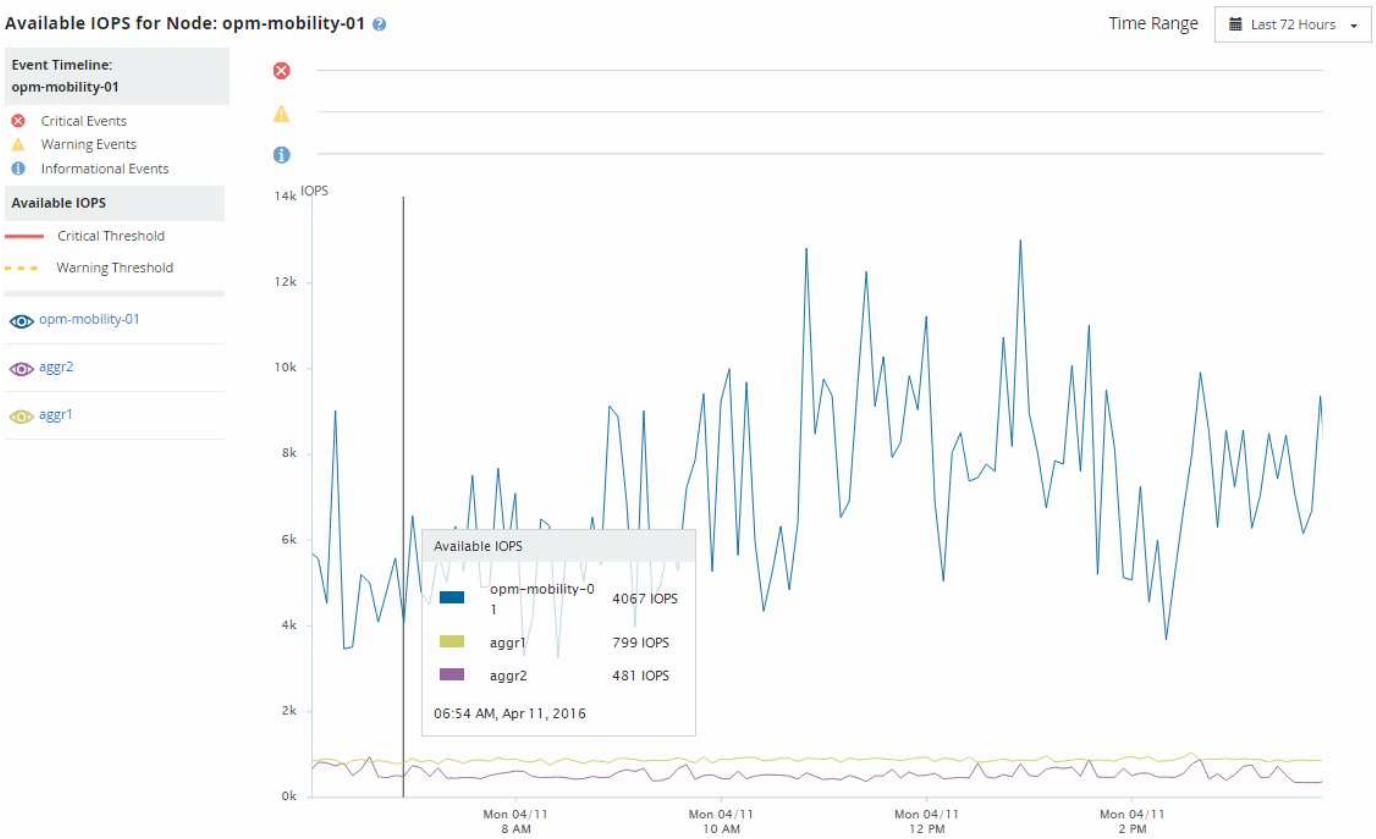
- Se algum nó ou agregado em quaisquer clusters tiver um valor alto de capacidade de desempenho usada
- Se algum nó ou agregado em qualquer cluster tem eventos ativos de capacidade de desempenho usada
- Os nós e agregados com o maior e o menor valor de capacidade de desempenho utilizada em um cluster
- Valores de latência e dos contadores de utilização em conjunto com nós ou agregados que apresentam valores altos de capacidade de desempenho utilizada
- Como os valores de capacidade de desempenho usada dos nós em um par de 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 usada

Visualize os valores de IOPS disponíveis para nós e agregados no Active IQ Unified Manager

Você pode monitorar os valores de IOPS disponíveis para todos os nós ou para todos os agregados em um cluster, ou pode visualizar detalhes para um único nó ou agregado.

Os valores de IOPS disponíveis aparecem nas páginas Performance Inventory e nos gráficos da página Performance Explorer para nós e agregados. Por exemplo, ao visualizar um nó na página Node/Performance Explorer, você pode selecionar o gráfico do contador “Available IOPS” na lista para comparar os valores de

IOPS disponíveis do nó e de vários agregados nesse nó.



Monitorar o contador de IOPS disponíveis permite identificar:

- Os nós ou agregados que têm os maiores valores de IOPS disponíveis ajudam a determinar onde implantar futuras cargas de trabalho.
- Os nós ou agregados que apresentam os menores valores de IOPS disponíveis permitem identificar os recursos que você deve monitorar para possíveis problemas de desempenho futuros.
- Os volumes e LUNs mais movimentados em um agregado que possui um pequeno valor de IOPS disponível.

Visualize os gráficos do contador de capacidade de desempenho no Active IQ Unified Manager

Você pode visualizar gráficos da capacidade de desempenho usada para nós e agregados na página Performance Explorer. Isso permite que você visualize dados detalhados da capacidade de desempenho dos nós e agregados selecionados em um período específico.

O gráfico de contador padrão exibe os valores de capacidade de desempenho utilizada para os nós ou agregados selecionados. O gráfico de contador de detalhamento exibe os valores totais de capacidade de desempenho para o objeto raiz, separados em uso com base em protocolos de usuário versus processos de sistema em segundo plano. Além disso, a quantidade de capacidade de desempenho livre também é mostrada.

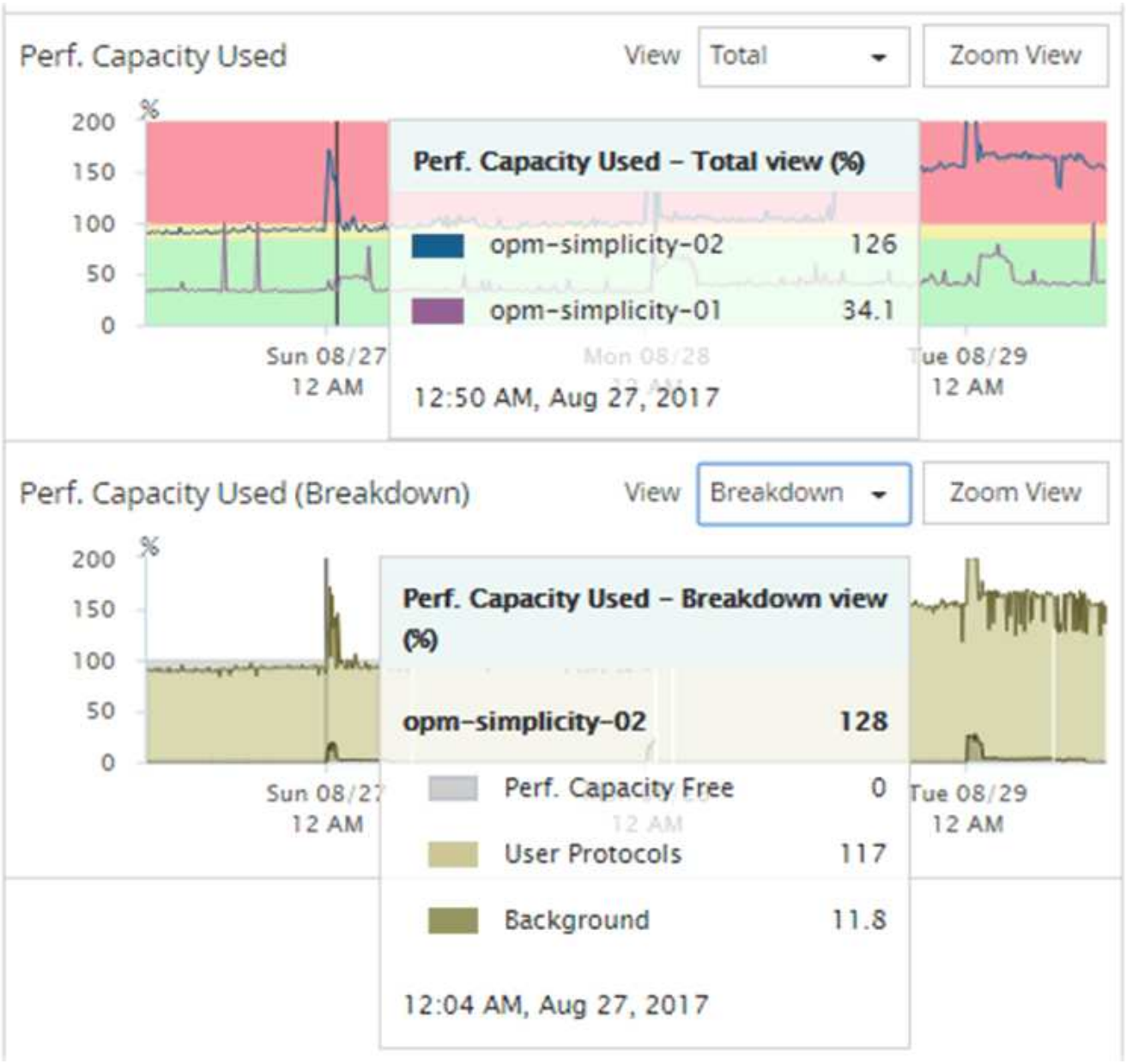
Como algumas atividades em segundo plano associadas ao gerenciamento do sistema e de dados são identificadas como cargas de trabalho do usuário e categorizadas como protocolos

de usuário, a porcentagem de protocolos de usuário pode parecer artificialmente alta quando esses processos são executados. Esses processos normalmente são executados por volta da meia-noite, quando o uso do cluster é baixo. Se você observar um pico na atividade de protocolos de usuário por volta da meia-noite, verifique se os trabalhos de backup do cluster ou outras atividades em segundo plano estão configurados para serem executados nesse horário.

Passos

1. Na página **Landing** de um nó ou agregado, selecione a aba **Explorer**.
2. No painel **Gráficos de contadores**, clique em **Escolher gráficos** e selecione o gráfico **Desemp. Capacidade usada**.
3. Deslize a tela para baixo até conseguir visualizar o gráfico.

   As cores do gráfico padrão mostram quando o objeto está na faixa ideal (amarelo), quando está subutilizado (verde) e quando está sobrecarregado (vermelho). O gráfico de detalhamento mostra informações detalhadas sobre a capacidade de desempenho apenas do objeto raiz.



4. Se você quiser visualizar qualquer um dos gráficos em tamanho real, clique em **Visualização ampliada**.

   Dessa forma, você pode abrir vários gráficos de contador em janelas separadas para comparar os valores de capacidade de desempenho usada com os valores de IOPS ou MBps durante o mesmo período.

Configure os limites de capacidade de desempenho utilizados no Active IQ Unified Manager

Você pode criar políticas de limite de desempenho definidas pelo usuário para acionar eventos quando o valor da capacidade de desempenho usada de um nó ou agregado exceder a configuração definida do limite de capacidade de desempenho usada.

Além disso, os nós podem ser configurados com uma política de limite de “takeover de capacidade de desempenho usada”. Essa política de limite totaliza as estatísticas de capacidade de desempenho usada de ambos os nós em um par de HA para determinar se algum 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 takeover de capacidade de desempenho usada pode ser aplicada a ambos os nós.

> Essa equivalência de capacidade de desempenho utilizada geralmente é válida entre os nós. No entanto, se houver um volume significativamente maior de tráfego entre nós destinado a um dos nós por meio de seu parceiro de failover, a capacidade de desempenho total utilizada ao executar todas as cargas de trabalho em um nó parceiro em comparação com o outro nó parceiro poderá ser ligeiramente diferente, dependendo de qual nó apresentou falha.

As condições de capacidade de desempenho utilizada também podem ser usadas como configurações de limite de desempenho secundárias para criar uma política de limite combinada ao definir limites para LUNs e volumes. A condição de capacidade de desempenho utilizada é aplicada ao agregado ou nó no qual o volume ou LUN reside. Por exemplo, você pode criar uma política de limite combinada usando os seguintes critérios:

Objeto de armazenamento	Contador de desempenho	Limiar de alerta	Limiar crítico	Duração
Volume	Latência	15 ms/op	25 ms/op	20 minutos
Agregado	Capacidade de desempenho utilizada	80%	95%	

As políticas de limite combinado geram um evento somente quando ambas as condições são ultrapassadas durante toda a duração.

Utilize o contador de capacidade de desempenho utilizada no Active IQ Unified Manager

Normalmente, as organizações querem operar com uma porcentagem de capacidade de desempenho usada abaixo de 100 para usar os recursos com eficiência e, ao mesmo tempo, reservar alguma capacidade de desempenho adicional para dar suporte às demandas dos períodos de pico. Você pode usar políticas de limiar para personalizar quando os alertas são enviados para valores altos de capacidade de desempenho usada.

Você pode estabelecer metas específicas com base nos seus requisitos de desempenho. Por exemplo, empresas de serviços financeiros podem reservar mais capacidade de desempenho para garantir a execução oportuna de negociações. Essas empresas podem definir limites de capacidade de desempenho utilizada na faixa de 70 a 80%. Empresas de manufatura com margens menores podem optar por reservar menos capacidade de desempenho se estiverem dispostas a sacrificar o desempenho para gerenciar melhor os custos de TI. Essas empresas podem definir limites de capacidade de desempenho utilizada na faixa de 85 a 95%.

Quando o valor da capacidade de desempenho utilizada 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 de 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 de carga de trabalho em seus nós e agregados.

Entenda e use a página Node Failover Planning

Utilize a página de Planejamento de Failover de Nós no Active IQ Unified Manager

A página de Planejamento de failover de nó/desempenho estima o impacto no desempenho de um nó caso o nó parceiro de alta disponibilidade (HA) falhe. O Unified Manager baseia as estimativas no desempenho histórico dos nós no par de HA.

Estimar o impacto de um failover no desempenho ajuda no planejamento para os seguintes cenários:

- Se um failover degradar consistentemente o desempenho estimado do nó que assume o controle a um nível inaceitável, você pode considerar adotar ações corretivas para reduzir o impacto no desempenho causado por um failover.
- Antes de iniciar um failover manual para executar tarefas de manutenção de hardware, você pode estimar como o failover afetará o desempenho do nó de takeover para determinar o melhor momento para executar a tarefa.

Determine as ações corretivas na página Planejamento de Failover de Desempenho/Nó no Active IQ Unified Manager

Com base nas informações exibidas na página Performance/Node Failover Planning, 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 em caso de failover, você pode mover alguns volumes ou LUNs de um nó no par de HA para outros nós no cluster. Isso garante que o nó primário possa continuar a fornecer um desempenho aceitável após um failover.

Analise os componentes da página de Planejamento de Failover de Desempenho/Nó no Active IQ Unified Manager

Os componentes da página Planejamento de failover de nó/desempenho são exibidos em uma grade e no painel de comparação. Essas seções permitem avaliar o impacto de um failover de nó no desempenho do nó que assume o controle.

Grade de estatísticas de desempenho

A página Performance/Node Failover Planning exibe uma tabela contendo estatísticas de latência, IOPS, utilização e capacidade de desempenho usada.

> Os valores de latência e IOPS exibidos nesta página e na página Performance/Node Performance Explorer podem não corresponder, porque contadores de desempenho diferentes são usados para calcular os valores e 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 ele falha. O objeto raiz é sempre o nó Primary.

- Parceiro

  O nó que falha no cenário de failover.

- Takeover estimado

  O mesmo que o nó primário. As estatísticas de desempenho exibidas para este nó mostram o desempenho do nó de takeover após ele assumir o parceiro com falha.

> Embora a carga de trabalho do nó de takeover seja equivalente à soma das cargas de trabalho de ambos os nós após um failover, as estatísticas do nó de takeover estimado 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 takeover estimado poderá ter uma latência de 4 ms/op. Esse valor é um cálculo que o Unified Manager realiza.

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 poderá clicar na guia **Failover Planning** para ver como o desempenho muda nesse cenário de falha de nó. Por exemplo, se Node1 for o nó primário e Node2 for o nó parceiro, você poderá clicar em Node2 para torná-lo o nó primário. Dessa forma, você poderá ver como o desempenho estimado muda dependendo de qual nó falha.

Painel de comparação

A lista a seguir descreve os componentes exibidos no painel Comparing por padrão:

- **Gráficos de eventos**

  Eles são exibidos no mesmo formato que os da página Performance/Node Performance Explorer. Eles se referem apenas ao nó primário.

- **Gráficos de contadores**

  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 qualquer momento.

  Por exemplo, suponha que o gráfico de Utilização mostre 73% para o nó de takeover estimado às 11h do dia 8 de fevereiro. Se tivesse ocorrido um failover naquele momento, a utilização do nó de takeover teria sido de 73%.

As estatísticas históricas ajudam você a encontrar o momento ideal para iniciar um failover, minimizando a possibilidade de sobrecarga do nó de takeover. Você pode agendar um failover somente nos momentos em que o desempenho previsto do nó de takeover for aceitável.

Por padrão, as estatísticas do objeto raiz e do nó parceiro são exibidas no painel Comparing. Diferentemente da página Performance/Node Performance Explorer, esta página não exibe o botão **Add** para você adicionar objetos para comparação de estatísticas.

Você pode personalizar o painel Comparação da mesma forma que faz na página Performance/Node Performance Explorer. A lista a seguir mostra exemplos de personalização dos gráficos:

- Clique no nome do nó para mostrar ou ocultar as estatísticas do nó nos gráficos de contador.
- Clique em **Zoom View** para exibir um gráfico detalhado de um determinado contador em uma nova janela.

Crie políticas de limite para o planejamento de failover de nós no Active IQ Unified Manager

Você pode criar uma política de limite de nó para receber uma notificação na página Performance/Node Failover Planning quando um possível failover degradar o desempenho do nó de takeover a um nível inaceitável.

A política de limite de desempenho definida pelo sistema, denominada “Node HA pair over-utilized”, gera um evento de aviso se o limite for ultrapassado por seis períodos de coleta consecutivos (30 minutos). O limite é considerado ultrapassado se a capacidade de desempenho combinada utilizada pelos nós em um par de HA exceder 200%.

O evento da política de limite definida pelo sistema alerta você para o fato de que um failover fará com que a latência do nó de takeover aumente para um nível inaceitável. Quando você vir um evento gerado por essa política para um nó específico, poderá navegar até a página Desempenho/Planejamento de Failover de 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 “Performance Capacity Used - Takeover” e, em seguida, aplicar a política aos nós selecionados. Especificar um limite inferior a 200% permite que você receba um evento antes que o limite da política definida pelo sistema seja ultrapassado. Você também pode especificar o período mínimo durante o qual o limite é excedido para menos de 30 minutos, caso queira ser notificado antes que o evento da política definida 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 dos nós em um par de HA exceder 175% por mais de 10 minutos. Você pode aplicar essa política a Node1 e Node2, que formam um par de HA. Após receber uma notificação de evento de aviso para Node1 ou Node2, você pode visualizar a página Performance/Node Failover Planning desse nó para avaliar o impacto estimado no desempenho no nó de takeover. Você pode tomar medidas corretivas para evitar sobrecarregar o nó de takeover se um failover realmente acontecer. Se você tomar medidas quando a capacidade de desempenho combinada usada dos nós estiver abaixo de 200%, a latência do nó de takeover não atingirá um nível inaceitável, mesmo que um failover aconteça durante esse período.

Utilize o gráfico de detalhamento da capacidade de desempenho utilizada para o planejamento de failover no Active IQ Unified Manager

O gráfico detalhado de detalhamento da capacidade de desempenho usada mostra a capacidade de desempenho usada pelo nó primário e pelo nó parceiro. Ele também

mostra a quantidade de capacidade de desempenho livre no nó de takeover estimado. Essas informações ajudam você a determinar se poderá haver um problema de desempenho caso o nó parceiro falhe.

Além de mostrar a capacidade de desempenho total utilizada pelos nós, o gráfico de detalhamento divide os valores de cada nó em protocolos de usuário e processos em segundo plano.

- Os protocolos de usuário são as operações de entrada/saída (I/O) de aplicativos do usuário de e para o cluster.
- Os processos em segundo plano são os processos internos do sistema envolvidos na eficiência de storage, na replicação de dados e na saúde do sistema.

Esse nível adicional de detalhamento permite que você determine se um problema de desempenho é causado pela atividade de aplicativos do usuário ou por processos do sistema em segundo plano, como deduplicação, reconstrução de RAID, limpeza de disco e cópias do SnapMirror.

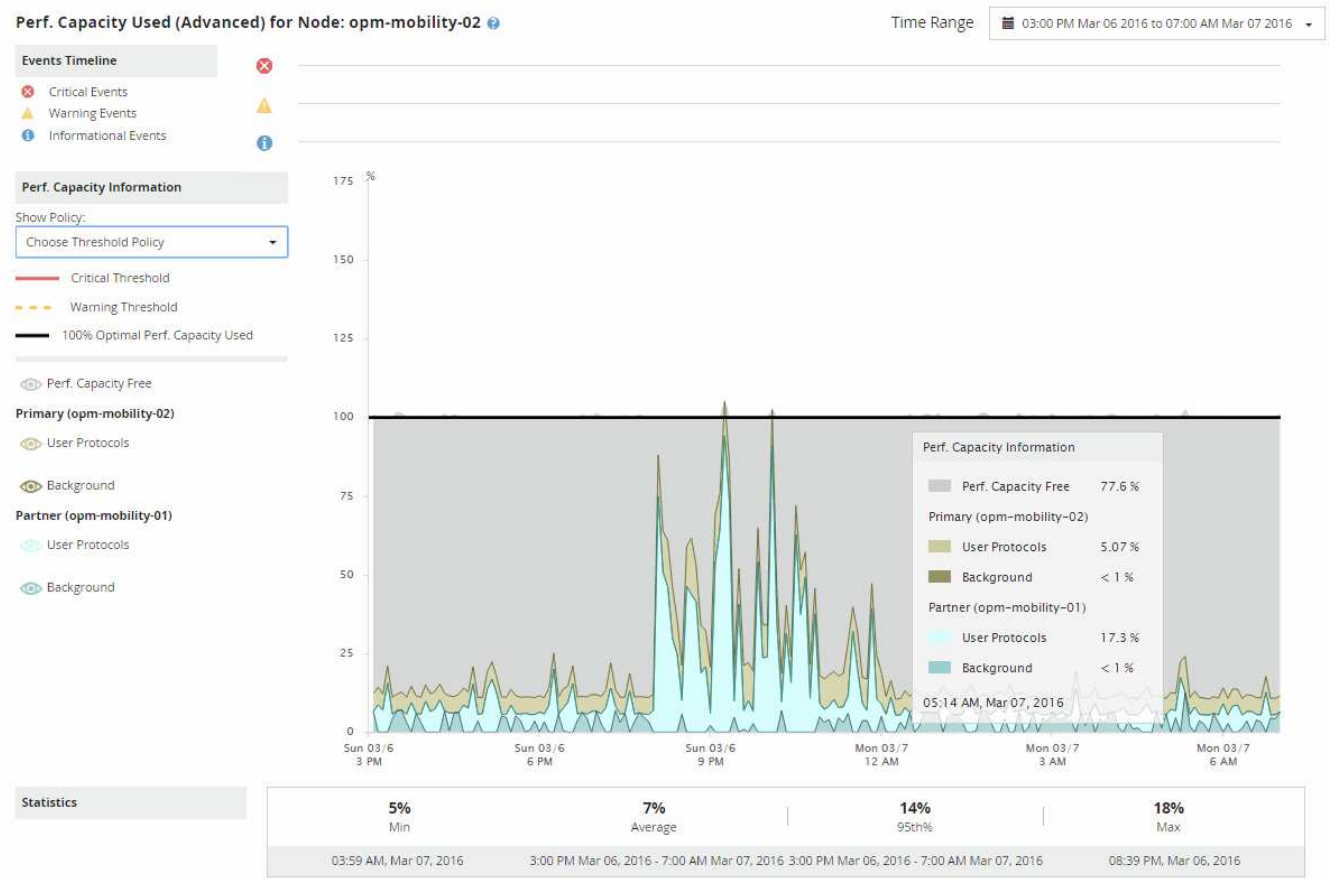
Passos

1. Acesse a página **Desempenho/Planejamento de failover de nó** do nó que servirá como o nó de takeover estimado.
2. No seletor **Intervalo de Tempo**, escolha o período para o qual as estatísticas históricas são exibidas na grade de contadores e nos gráficos de contadores.

   São exibidos os gráficos de contadores com estatísticas do nó Primary, do nó Partner e do nó Estimated Takeover.

3. Na lista **Escolher gráficos**, selecione **Desemp. Capacidade usada**.
4. No gráfico **Desempenho da Capacidade Utilizada *, selecione *Detalhamento** e clique em **Visualização Ampliada**.

   O gráfico detalhado da capacidade de desempenho Usada é exibido.



5. Mova o cursor sobre o gráfico detalhado para visualizar as informações sobre a capacidade de desempenho utilizada na janela pop-up.

   A porcentagem de capacidade livre de des Empenho é a capacidade de desempenho disponível no nó de takeover estimado. Ela indica quanta capacidade de desempenho resta no nó de takeover após um failover. Se for 0%, um failover fará com que a latência aumente para um nível inaceitável no nó de takeover.

6. Considere tomar medidas corretivas para evitar uma baixa porcentagem de capacidade de desempenho livre.

   Se você planeja iniciar um failover para manutenção do nó, escolha um momento para fazer failover do nó parceiro quando a porcentagem de capacidade de desempenho livre não estiver em 0.

Coletar dados e monitorar o desempenho da carga de trabalho

Colete dados e monitore o desempenho da carga de trabalho no Active IQ Unified Manager

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. O Unified Manager retém no máximo 30 dias de dados históricos de desempenho e eventos em intervalos de 5 minutos e usa esses dados para prever a faixa de latência esperada para todas as cargas de trabalho monitoradas.

O Unified Manager precisa coletar no mínimo 3 dias de atividade da carga de trabalho antes de poder iniciar a análise e antes que a previsão de latência para o tempo de resposta de I/O possa ser exibida na página Workload Analysis e na página Event details. Enquanto essa atividade é coletada, a previsão de latência não exibe todas as alterações decorrentes da 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 tiverem se passado mais de 24 horas 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 estarão disponíveis.

> O horário de verão altera a hora do sistema, o que modifica 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 usando o Unified Manager, mas, como o Unified Manager usa a previsão de latência para detectar eventos dinâmicos, alguns eventos podem não ser precisos. Os eventos detectados antes da mudança de horário não são afetados.

Monitore os tipos de carga de trabalho com o Active IQ 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 os processos envolvidos em solicitações de leitura e gravação. Um volume, uma LUN, um compartilhamento NFS, um 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:

  - Trata-se de uma cópia de proteção de dados (DP) em modo somente leitura. (Os volumes DP são monitorados quanto ao tráfego gerado pelo usuário.)
  - Trata-se de um clone de dados offline.
  - Trata-se de um volume espelhado em uma configuração MetroCluster.
- ***Cargas de trabalho definidas pelo sistema***

  Os processos internos envolvidos na eficiência de storage, replicação de dados e integridade do sistema, incluindo:

  - Eficiência de storage, como a deduplicação
  - 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

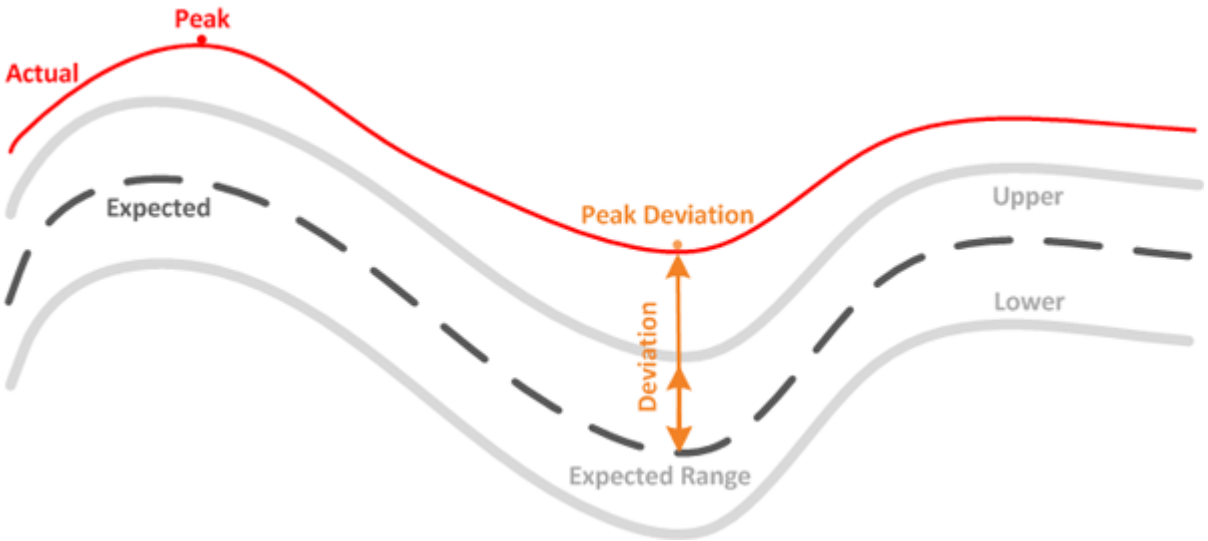
- Saúde do sistema de arquivos, que inclui várias atividades do WAFL
- Scanners do sistema de arquivos, como WAFL scan
- Descarregamento de cópias, como operações de eficiência de storage descarregadas de hosts VMware
- Saúde do sistema, como movimentação de volumes, compressão de dados e assim por diante
- 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, não é possível pesquisar o nome de uma carga de trabalho definida pelo sistema para visualizar seus dados de desempenho na GUI.

Compreenda os valores de medição de desempenho da carga de trabalho no Active IQ Unified Manager

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 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 apresenta o desempenho esperado aciona um evento de desempenho dinâmico para notificar você.

Na ilustração a seguir, o valor real, em vermelho, representa as estatísticas reais de desempenho no período analisado. O valor real ultrapassou o limite de desempenho, que é o limite superior da previsão de latência. O pico representa o maior valor real no período analisado. O desvio mede a diferença entre os valores esperados (a previsão) e os valores reais, sendo que o desvio máximo indica a maior diferença entre os valores esperados e os valores reais.



A tabela a seguir lista os valores de medição do desempenho da carga de trabalho.

Medição	Descrição
Atividade	A porcentagem do limite de QoS utilizada pelas cargas de trabalho no grupo de políticas. Se o Unified Manager detectar uma alteração em um grupo de políticas, como a adição ou remoção de um volume ou a alteração do limite de QoS, os valores reais e esperados podem exceder 100% do limite definido. Se um valor exceder 100% do limite definido, ele será exibido como >100%. Se um valor for inferior a 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 diferença entre os valores esperados e os valores reais. É a razão entre o valor real menos o valor esperado e o valor máximo do intervalo esperado menos o valor esperado. Um valor de desvio negativo indica que o desempenho da carga de trabalho é inferior ao esperado, enquanto um valor de desvio positivo indica que o desempenho da carga de trabalho é superior ao esperado.
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 a faixa esperada (previsão de latência) de valores.
Previsão de latência (faixa esperada)	A previsão de latência é uma estimativa dos valores superior e inferior 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 durante 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.

Medição	Descrição
Utilização	Para os componentes de processamento de rede, processamento de dados e agregação, a porcentagem do tempo em que ficam ocupados para concluir operações de carga de trabalho durante um período de tempo. Por exemplo, a porcentagem de tempo de que os componentes de processamento de rede ou de processamento de dados precisam para processar uma solicitação de E/S ou de que um agregado precisa para atender a uma solicitação de leitura ou gravação.
Taxa de transferência de gravação	A 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 do MetroCluster.

Entenda como o Active IQ Unified Manager calcula a faixa de desempenho esperada

A previsão de latência é uma estimativa dos valores superior e inferior 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 da carga de trabalho no storage de back-end durante esse período. Os funcionários podem notar lentidão no tempo de resposta de seus clientes de e-mail.

Durante o horário de almoço, entre 12h e 13h, e no final do expediente, após as 17h, a maioria dos funcionários provavelmente está longe de seus computadores. A demanda nos servidores de e-mail normalmente diminui, reduzindo também a demanda no storage de back-end. Como alternativa, pode haver operações de carga de trabalho agendadas, como backups de storage ou verificação de vírus, que começam após as 17h e aumentam a atividade no storage de back-end.

Ao longo de vários dias, o aumento e a diminuição da atividade da carga de trabalho determinam a faixa esperada de atividade (previsão de latência), com limites superiores e inferiores para uma carga de trabalho. Quando a atividade real da carga de trabalho de um objeto está fora dos limites superiores ou inferiores e permanece fora desses limites por um período de tempo, isso pode indicar que o objeto está sendo sobrecarregado ou subutilizado.

Como a previsão de latência é criada

O Unified Manager precisa coletar no mínimo 3 dias de atividade da 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 de dados mínima necessária não considera todas as alterações decorrentes da 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 altera a hora do sistema, o que modifica 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 usando o Unified Manager, mas, como o Unified Manager usa a previsão de latência para detectar eventos dinâmicos, alguns eventos podem não ser precisos. Os eventos detectados antes da mudança de horário não são afetados.

Utilize a previsão de latência para análise de desempenho no Active IQ Unified Manager

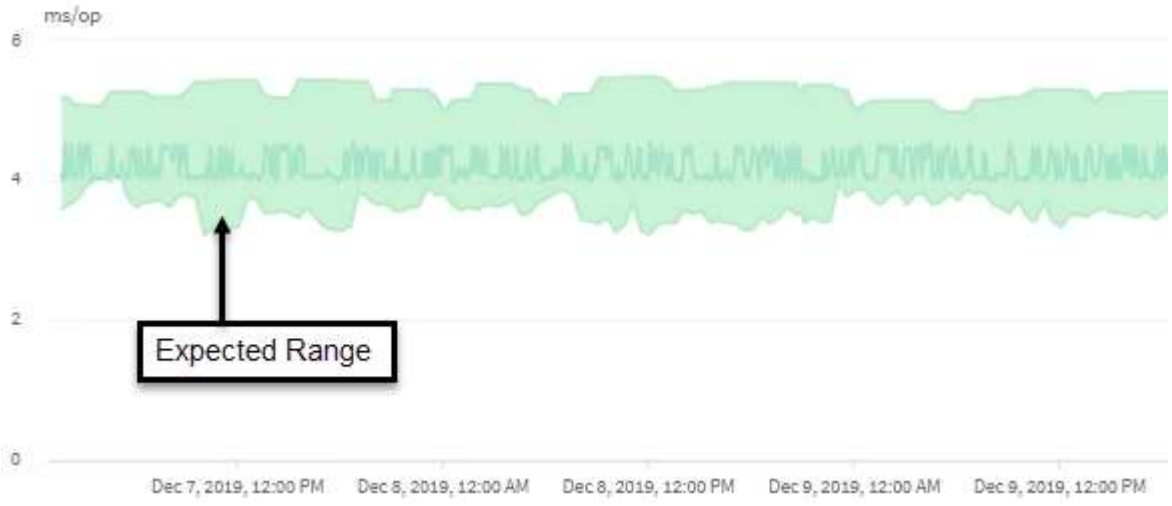
O Unified Manager usa a previsão de latência para representar a atividade típica de latência de E/S (tempo de resposta) para suas cargas de trabalho monitoradas. Ele alerta você quando a latência real de uma carga de trabalho está acima dos limites superiores da previsão de latência, o que aciona um 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. Ao longo do tempo, o Unified Manager aprende com as medições de desempenho anteriores para prever os níveis esperados de desempenho e atividade para a carga de trabalho. O limite superior da faixa esperada 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 da faixa esperada. 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 fica alta e a carga de trabalho apresenta desempenho inferior ao esperado. O desempenho de outras cargas de trabalho que compartilham os mesmos componentes do cluster também pode ser inferior ao esperado.

O Unified Manager analisa o evento de violação de limite e determina se a atividade é um evento de desempenho. Se a atividade elevada da carga de trabalho permanecer consistente por um longo período, como várias horas, o Unified Manager considera a atividade normal e ajusta dinamicamente a previsão de latência para formar o novo limite dinâmico de desempenho.

Algumas cargas de trabalho podem ter atividade consistentemente baixa, em que a previsão de latência para a latência não apresenta uma alta taxa de alteração ao longo do tempo. Para minimizar o número de eventos durante a análise de eventos de desempenho, o Unified Manager aciona um evento apenas para volumes de baixa atividade cujas operações e latências sejam 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 valor mais baixo e de 5,5 ms/op no 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 à contenção em um componente do cluster, ela ficará acima da previsão de latência e terá excedido o limite de desempenho dinâmico.

Quando o tráfego de rede diminui ou o componente do cluster deixa de estar em contenção, a latência retorna à previsão de latência. Se a latência permanecer em ou acima de 10 ms/op por um longo período, talvez seja necessário tomar medidas corretivas para resolver o evento.

Use a latência da carga de trabalho para identificar problemas de desempenho no Active IQ Unified Manager

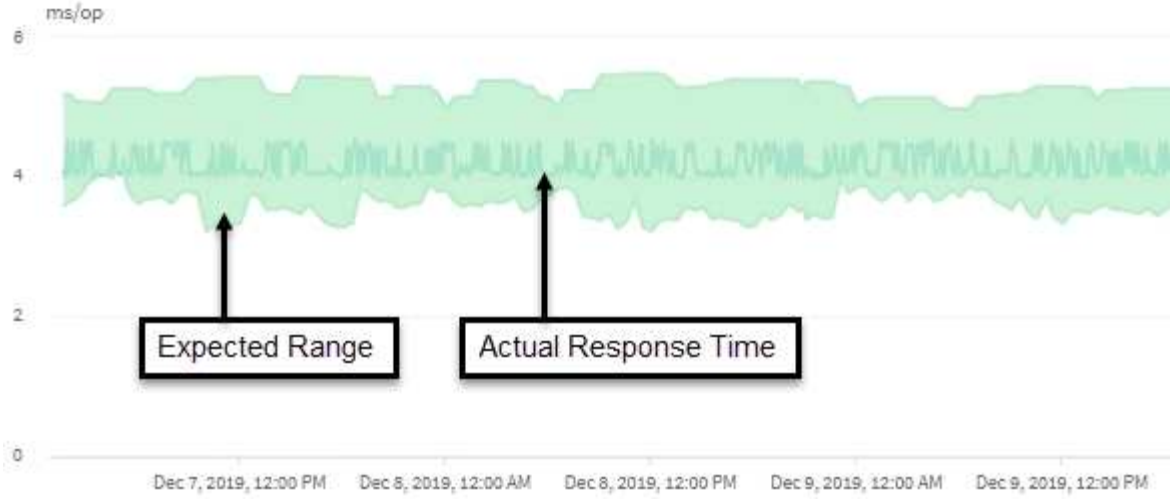
A latência da carga de trabalho (tempo de resposta) é o tempo que um volume em um cluster leva para responder às solicitações de E/S de aplicativos cliente. O Unified Manager usa a latência para detectar e alertar você sobre eventos de desempenho.

Uma alta latência significa que as solicitações de aplicativos para um volume em um cluster estão demorando mais do que o normal. A causa da alta latência pode estar no próprio cluster, devido à contenção em um ou mais componentes do cluster. A alta latência também pode ser causada por problemas 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 a deduplicação, que aumentam a demanda por componentes do cluster compartilhados por outras cargas de trabalho também podem contribuir para alta latência. Se a latência real exceder o limite dinâmico de desempenho da faixa esperada (previsão de latência), o Unified Manager analisará o evento para determinar se é um evento de desempenho que talvez você precise resolver. A latência é medida em milissegundos por operação (ms/op).

No gráfico Latency Total na página Workload Analysis, você pode ver 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 você a determinar quais operações têm a maior atividade ou se operações específicas apresentam 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 de workload específicas ou os componentes do cluster envolvidos no evento.



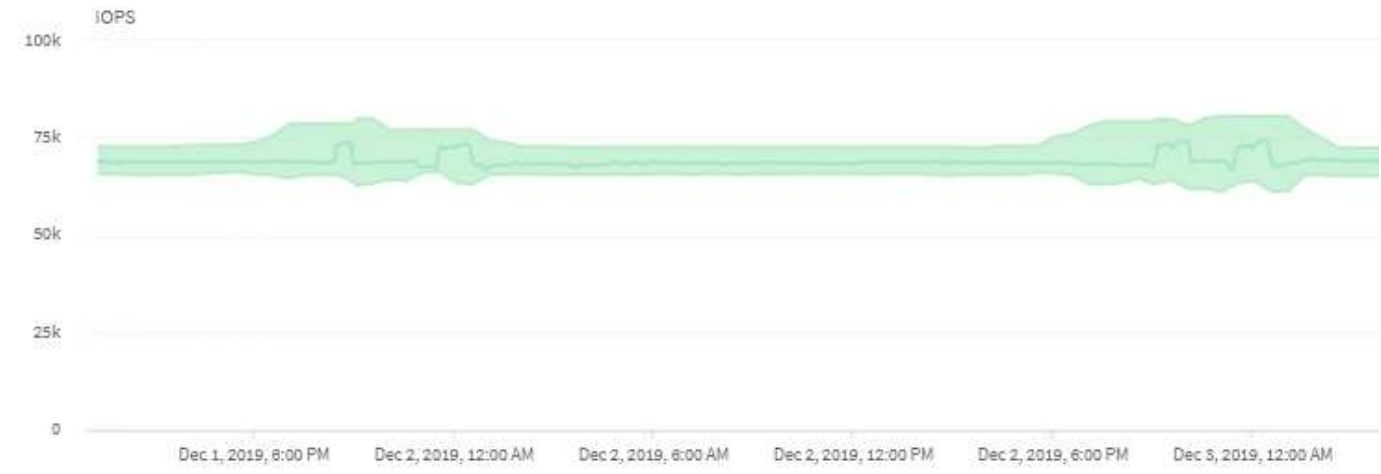
Este exemplo mostra o gráfico de latência. A atividade real do tempo de resposta (latência) é representada por uma linha azul, e a previsão de latência (intervalo esperado) é representada em verde.

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 foi desligado durante esse período ou a coleta demorou mais do que o período de coleta de 5 minutos.

Avalie como as operações de cluster podem afetar a latência no Active IQ Unified Manager

As 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 você a determinar se os processos do cluster, como a criação de backups ou a execução de 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 de carga de trabalho específicas que podem ter sido as principais responsáveis pelo evento de desempenho. As IOPS são medidas em operações por segundo (ops/sec).



Este exemplo mostra o gráfico de IOPS. As estatísticas reais de operações são representadas por uma linha

azul, e a previsão de IOPS das estatísticas de operações é representada pela linha 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 estatísticas suficientes não foram coletadas para o Unified Manager analisar. Você precisa reduzir os recursos que o cluster está usando para que estatísticas possam ser coletadas.

Monitore o desempenho do MetroCluster com o Active IQ Unified Manager

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 causando altos tempos de resposta de E/S em outros volumes do cluster local, o Unified Manager acionará eventos de desempenho para notificar você.

> 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 do MetroCluster espelha seus dados para o cluster parceiro, os dados são gravados na NVRAM e, em seguida, transferidos pelos links entre switches (ISLs) para os agregados remotos. O Unified Manager analisa a NVRAM para identificar as cargas de trabalho cuja alta taxa de transferência de gravação está sobrecarregando a NVRAM, colocando a NVRAM em contenção.

As cargas de trabalho cujo desvio no tempo de resposta excedeu o limite de desempenho são chamadas de *vítimas*, e as cargas de trabalho cujo desvio na taxa de transferência de gravação na NVRAM é maior que o normal, causando a contenção, são chamadas de *agressoras*. Como apenas as solicitações de gravação são espelhadas para o cluster 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 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 à esquerda:

- visualização **Armazenamento > Clusters > Desempenho: todos os Clusters**. Consulte
- **Armazenamento > Volumes > Desempenho: visualização de 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 afetadas envolvidas em um evento de desempenho"

"Identificação das cargas de trabalho agressoras envolvidas em um evento de desempenho"

"Identificação das cargas de trabalho shark envolvidas em um evento de desempenho"

Compreenda os eventos e alertas de desempenho

Compreenda os eventos e alertas de desempenho no Active IQ Unified Manager

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 eventos de integridade 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 múltiplas ocorrências da mesma condição de evento para o mesmo componente de cluster, ele trata todas as ocorrências como um único evento, e não como eventos separados.

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

Identifique as fontes de eventos de desempenho no Active IQ Unified Manager

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 integridade 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, como agregados e volumes, para que eventos sejam gerados quando um valor de limite para um contador de desempenho for ultrapassado.

  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 baseados em valores de limite definidos pelo sistema. Essas políticas de limite estão incluídas na instalação do Unified Manager para solucionar problemas de desempenho comuns.

  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 resultantes de falhas ou erros na infraestrutura de TI, ou de cargas de trabalho que sobrecarregam os recursos do cluster. A causa desses eventos pode ser um problema simples que se corrige com o 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 compartilhados do cluster.

Esses limites estão ativados por padrão, e você poderá ver eventos após três dias de coleta de dados de um novo cluster.

Priorize eventos de desempenho por gravidade no Active IQ Unified Manager

Cada evento de desempenho está 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 medidas corretivas não forem tomadas 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 podem não exigir ação corretiva imediata.

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

- **Informação**

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

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

Para obter mais informações, consulte os seguintes links:

- "O que acontece quando um evento é recebido"
- "Que informações estão contidas em um e-mail de alerta"
- "Adicionando alertas"
- "Adicionando alertas para eventos de desempenho"

Monitore as alterações de configuração detectadas pelo Active IQ 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 consultar os gráficos de desempenho nas páginas do Explorador de Desempenho e na página de Análise de Carga de Trabalho para verificar se o evento de alteração afetou o desempenho do objeto de

cluster selecionado. Se a alteração foi detectada simultaneamente ou em um momento próximo a um evento de desempenho, ela pode ter contribuído para o problema que acionou o alerta.

O Unified Manager pode detectar os seguintes eventos de alteração, que são categorizados como eventos informativos:

- Um volume se desloca entre agregados.

  O Unified Manager consegue detectar quando a movimentação está em andamento, concluída ou falhou. Se o Unified Manager estiver inativo durante uma movimentação de volume, ao retornar, ele detectará a movimentação e exibirá um evento de alteração correspondente.

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

- Um nó em um par de HA assume o controle ou faz o giveback do armazenamento do nó parceiro.

  O Unified Manager consegue detectar quando a operação de tomada de controle, tomada de controle parcial ou giveback foi concluída. Se a tomada de controle for causada por um nó em pânico, o Unified Manager não detectará o evento.

- Uma operação de atualização ou reversão do ONTAP é concluída com sucesso.

  A versão anterior e a nova versão são exibidas.

Compreenda as políticas de limite de desempenho definidas pelo sistema no Active IQ Unified Manager

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

As políticas de limite de desempenho definidas pelo sistema não estão habilitadas nos sistemas Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select.

Se você estiver recebendo eventos desnecessários de políticas de limite de desempenho definidas pelo sistema, poderá desativar os eventos de políticas individuais na página Configuração de eventos.

Políticas de limite do cluster

As políticas de limite de desempenho de cluster definidas pelo sistema são atribuídas, por padrão, a todos os clusters monitorados pelo Unified Manager:

- **Desequilíbrio de carga no 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 das cargas de trabalho.

Isso ocorre ao comparar o valor de capacidade de desempenho usada de todos os nós em um cluster para verificar se algum nó excedeu o valor limite de 30% por mais de 24 horas. Este é um evento de aviso.

- **Desequilíbrio na capacidade do cluster**

  Identifica situações em que um agregado tem uma capacidade utilizada muito maior do que outros agregados no cluster, afetando potencialmente o espaço necessário para as operações.

  Isso é feito comparando o valor da capacidade utilizada de todos os agregados no cluster para verificar se há uma diferença de 70% entre quaisquer agregados. Isso é um evento de aviso.

Políticas de limite de nós

As políticas de limite de desempenho de nó definidas pelo sistema são atribuídas, por padrão, a todos os nós 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.

  Isso é feito procurando nós que estejam utilizando mais de 100% de sua capacidade de desempenho por mais de 12 horas. Isso é um evento de alerta.

- **Par de HA do nó sobrecarregado**

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

  Isso é feito analisando o valor da capacidade de desempenho utilizada dos dois nós no par de HA. Se a capacidade de desempenho combinada utilizada dos dois nós exceder 200% por mais de 12 horas, um failover de controladora afetará as latências da carga de trabalho. Este é um evento informativo.

- **Fragmentação de disco do nó**

  Identifica situações em que um ou mais discos em um agregado estão fragmentados, o que pode prejudicar o desempenho de serviços essenciais do sistema e afetar a latência da carga de trabalho em um nó.

  Isso é feito analisando determinadas proporções de operações de leitura e de gravação em todos os agregados de um nó. Essa política também pode ser acionada durante a ressincronização do SyncMirror ou quando erros são encontrados durante operações de limpeza de disco. Isso é um evento de aviso.

  > A política “Fragmentação de disco do nó” analisa agregados compostos apenas por HDDs; os agregados do Flash Pool, de SSD e do FabricPool não são analisados.

Políticas de limiar agregado

A política de limite de desempenho agregado definida pelo sistema é atribuída por padrão a todos os agregados nos clusters monitorados pelo Unified Manager:

- **Discos do agregado superutilizados**

  Identifica situações em que um agregado está operando acima dos limites de sua eficiência operacional, afetando potencialmente as latências da carga de trabalho. Identifica essas situações procurando

agregados nos quais os discos no agregado estejam com mais de 95% de utilização por mais de 30 minutos. Essa política multicondição realiza então a seguinte análise para ajudar a determinar a causa do problema:

- Há algum disco no agregado que esteja 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 reparidade.

- Existe algum gargalo de comunicação na interconexão Fibre Channel da gaveta de discos?
- 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 estiverem com mais de 95% de utilização.

A política “Aggregate disks over-utilized” analisa agregados compostos apenas por HDD e agregados do Flash Pool (híbridos); os agregados de SSD e do FabricPool não são analisados.

Políticas de limite de latência da 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 “expected latency” definido:

- **Limite de latência de volume/LUN da carga de trabalho ultrapassado 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 aviso.

  Isso ocorre ao procurar cargas de trabalho que excederam o valor de latência esperado durante 30% do tempo na 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 do 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 IOPS ou MB/s para QoS**

  Identifica volumes e LUNs que excederam o limite máximo de IOPS ou de taxa de transferência em MB/s do QoS e que estão afetando a latência da carga de trabalho. Este é um evento de aviso.

  Quando uma única carga de trabalho é atribuída a um grupo de políticas, isso ocorre procurando 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 somando os IOPS ou MB/s de todas as cargas de trabalho da política e verificando esse total em relação ao limite.

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

Identifica volumes que excederam o limite de taxa de transferência de pico de IOPS/TB do 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 aviso.

Ele faz isso convertendo o limite de pico de IOPS/TB definido na política de QoS adaptável em um valor de IOPS máximo 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.

Essa política se aplica a volumes somente quando o cluster é instalado com o software ONTAP 9.3 ou 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, o sistema procura volumes que excederam o valor máximo de QoS em MB/s durante cada período de coleta de desempenho na hora anterior.

Essa política se aplica a volumes somente quando o cluster é instalado com o software ONTAP 9.5 ou posterior.

Analise eventos de desempenho e notificações no Active IQ Unified Manager

Os 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 representa um problema que você precisa resolver.

O Unified Manager monitora a latência de I/O (tempo de resposta) e IOPS (operações) dos volumes em um cluster. Quando outras cargas de trabalho usam excessivamente um componente do cluster, por exemplo, o componente entra em contenção e não consegue operar em um nível ideal para atender às demandas da carga de trabalho. O desempenho de outras cargas de trabalho que usam o mesmo componente pode ser afetado, fazendo com que suas latências aumentem. Se a latência ultrapassar o limite de desempenho dinâmico, o Unified Manager aciona um evento de desempenho para notificar você.

Análise de eventos

O Unified Manager realiza as seguintes análises, usando as estatísticas de desempenho dos 15 dias anteriores, para identificar as cargas de trabalho vítimas, as cargas de trabalho agressoras e o componente do cluster envolvido em um evento:

- Identifica as cargas de trabalho afetadas 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 do Flash Pool (camada local), os eventos são acionados somente quando a latência é superior a 5 milissegundos (ms) e as IOPS são superiores a 10 operações por segundo (ops/sec).
  - Para volumes em agregados totalmente SSD ou agregados do FabricPool (camada de nuvem), os eventos são acionados somente quando a latência é maior que 1 ms e as IOPS são superiores a 100 operações/seg.
- Identifica o componente do cluster em contenção.

Se a latência das cargas de trabalho vítimas na interconexão de cluster for superior a 1 ms, o Unified Manager considera isso significativo e aciona um evento para a interconexão de cluster.

- Identifica as cargas de trabalho agressoras que estão usando excessivamente o componente do cluster e fazendo com que ele entre em contenção.
- Classifica as cargas de trabalho envolvidas, com base no desvio na utilização ou atividade de um componente do cluster, para determinar quais cargas de trabalho agressivas apresentam a maior variação no uso do componente do cluster e quais cargas de trabalho afetadas são as mais impactadas.

Um evento pode ocorrer por um breve instante e se corrigir assim que o componente que está utilizando deixar de estar em disputa. Um evento contínuo é aquele que se repete para o mesmo componente do cluster dentro de um intervalo de cinco minutos e permanece no estado ativo. Para eventos contínuos, o Unified Manager dispara 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 para um volume. Cada evento possui um ID exclusivo que identifica o tipo de evento e os volumes, o cluster e os componentes do cluster envolvidos.

Um único volume pode estar envolvido em mais de um evento simultaneamente.

Estado do evento

Os eventos podem estar em um dos seguintes estados:

- **Ativo**

  Indica que o evento de desempenho está atualmente ativo (novo ou reconhecido). O problema que causou o evento não foi corrigido ou 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 se corrigiu sozinho ou foi 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 Dashboard e em muitas outras páginas da interface de usuário, e alertas para esses eventos são enviados para os endereços de e-mail especificados. Você pode visualizar informações detalhadas de análise sobre um evento e obter sugestões para resolvê-lo na página Event details e na página Workload Analysis.

Interação de eventos

Na página Event details e na página Workload Analysis, você pode interagir com os eventos das seguintes maneiras:

- Ao passar o mouse sobre um evento, uma mensagem é exibida mostrando a data e a hora em que o evento foi detectado.

  Se houver vários eventos para o mesmo período, a mensagem mostrará o número de eventos.

- Quando você clica em um único evento, uma caixa de diálogo mostra informações mais detalhadas sobre o evento, incluindo os componentes do cluster envolvidos.

  O componente em disputa está circulado e destacado em vermelho. Você pode clicar em **View full analysis** para visualizar a análise completa na página Event details. Se houver vários eventos para o mesmo período, a caixa de diálogo exibirá detalhes sobre os três eventos mais recentes. Você pode clicar em um evento para visualizar a análise do evento na página Event details.

Entenda como o Active IQ Unified Manager determina o impacto no desempenho de um evento

O Unified Manager utiliza 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 de detalhes do evento.

O Unified Manager compara os últimos valores analisados para uma carga de trabalho com o intervalo esperado de valores (previsão de latência). 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 fica 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 fica em torno de 15 ms/op. Ambas as cargas de trabalho estão bem dentro de sua previsão de latência. Devido à contenção no cluster, a latência de ambas as cargas de trabalho aumenta para 40 ms/op, ultrapassando o limite dinâmico de desempenho, que é o limite superior da previsão de latência, e acionando eventos. O desvio de latência, dos valores esperados para os valores acima do limite de desempenho, para a Carga de Trabalho A é de cerca de 33 ms/op, e o desvio para a Carga de Trabalho B é de cerca de 25 ms/op. A latência de ambas as cargas de trabalho atinge um pico de 40 ms/op, mas a Carga de Trabalho A teve o maior impacto no desempenho porque apresentou o maior desvio de latência, de 33 ms/op.

Na página de detalhes do evento, na seção Diagnóstico do sistema, você pode classificar as cargas de trabalho por desvio na atividade, utilização ou taxa de transferência de um componente do cluster. Você também pode classificar as cargas de trabalho por latência. Ao selecionar 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 das cargas de trabalho. Para a latência, os pontos vermelhos (🔴) indicam o cruzamento de um limite de desempenho por uma carga de trabalho afetada e o impacto subsequente na latência. Cada ponto vermelho indica um nível mais alto de desvio na latência, o que ajuda você a identificar as cargas de trabalho afetadas cuja latência foi mais impactada por um evento.

Compreenda os componentes do cluster e a contenção no Active IQ Unified Manager

Você pode identificar problemas de desempenho no cluster quando um componente entra em contenção. O desempenho das cargas de trabalho que usam o componente diminui, e o tempo de resposta (latência) às solicitações do cliente aumenta, o que aciona um evento no Unified Manager.

Um componente que está em contenção não consegue operar em seu nível ideal. Seu desempenho diminuiu,

e o desempenho de outros componentes e cargas de trabalho do cluster, chamados de *vítimas*, pode ter aumentado a latência. Para tirar um componente da contenção, é necessário reduzir sua carga de trabalho ou aumentar sua capacidade de lidar com mais trabalho, para que o desempenho retorne 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 storage pode estar sob contenção 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 afetadas, causando queda no desempenho. Para reduzir a quantidade de atividade no agregado, há diferentes medidas que você pode tomar, 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 sofram mais limitação.

O Unified Manager monitora os seguintes componentes do cluster para alertar você quando eles estiverem em contenção:

- **Rede**

  Representa o tempo de espera das solicitações de E/S pelos protocolos de rede externos no cluster. O tempo de espera é o tempo gasto aguardando a conclusão das transações “transfer ready” antes que o cluster possa responder a uma solicitação de E/S. Se o componente de rede estiver em contenção, isso significa que um alto tempo de espera na camada de protocolo está impactando a latência de uma ou mais cargas de trabalho.

- **Processamento de rede**

  Representa o componente de software no cluster envolvido no processamento de E/S entre a camada de protocolo e o cluster. O nó responsável pelo processamento de 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 ativo-ativo, o valor da latência de processamento de rede é exibido para ambos os nós, para que você possa verificar se os nós estão compartilhando a carga igualmente.

- **Limite máximo de QoS**

  Representa a configuração de taxa de transferência máxima (pico) do grupo de políticas de Qualidade de Serviço (QoS) de storage 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 têm a taxa limitada pelo limite de taxa de transferência definido, o que afeta a latência de uma ou mais dessas cargas de trabalho.

- **Limite mínimo de QoS**

  Representa a latência para uma carga de trabalho causada pela configuração mínima (esperada) de taxa de transferência de QoS atribuída a outras cargas de trabalho. Se a configuração mínima de QoS em determinadas cargas de trabalho utilizar a maior parte da largura de banda para garantir a taxa de transferência prometida, outras cargas de trabalho terão sua largura de banda limitada e apresentarão maior latência.

- **Interconexão de cluster**

Representa os cabos e adaptadores com os quais os nós em cluster estão fisicamente conectados. Se o componente de interconexão de cluster estiver em disputa, isso significa que o alto tempo de espera para solicitações de E/S na interconexão de 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 storage que contém a carga de trabalho. O nó que lida com 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 por Volume**

  Representa o processo que monitora o uso de todos os volumes ativos. Em ambientes de grande porte, com mais de 1000 volumes ativos, esse processo monitora quantos volumes críticos precisam acessar recursos por meio do nó simultaneamente. Quando o número de volumes ativos simultâneos excede o limite máximo recomendado, alguns dos volumes não críticos apresentarão latência conforme identificado aqui.

- **MetroCluster Recursos**

  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 do MetroCluster estiver em contenção, isso significa que uma alta taxa de transferência de gravação das cargas de trabalho no cluster local ou um problema na integridade do link está afetando a latência de uma ou mais cargas de trabalho no cluster local. Se o cluster não estiver em uma configuração do MetroCluster, este ícone não será exibido.

- **Operações de agregado ou agregado SSD**

  Representa o agregado de storage no qual as cargas de trabalho estão em execução. Se o componente de 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 em uma combinação de HDDs e SSDs (um agregado Flash Pool), ou em uma combinação de HDDs e uma camada de nuvem (um agregado FabricPool). Um “SSD Aggregate” consiste em todos os SSDs (um agregado all-flash), ou em uma combinação de SSDs e uma camada de nuvem (um agregado FabricPool).

- **Latência na nuvem**

  Representa o componente de software no cluster envolvido no processamento de E/S entre o cluster e a camada de nuvem na qual os dados de usuário são armazenados. Se o componente de latência da nuvem estiver em contenção, isso significa que uma grande quantidade de leituras de volumes hospedados na camada de nuvem está afetando a latência de uma ou mais cargas de trabalho.

- **Sincronização do SnapMirror**

  Representa o componente de software no cluster envolvido na replicação de dados de usuário do volume primário para o volume secundário em uma relação síncrona do SnapMirror. Se o componente de sincronização do SnapMirror estiver em contenção, isso significa que a atividade das operações síncronas do SnapMirror está afetando a latência de uma ou mais cargas de trabalho.

Identifique funções de carga de trabalho em eventos de desempenho no Active IQ Unified Manager

O Unified Manager utiliza funções para identificar o envolvimento de uma carga de trabalho em um evento de desempenho. As funções incluem vítimas, agressores e sharks. Uma carga de trabalho definida pelo usuário pode ser, ao mesmo tempo, vítima, agressora e shark.

Papel	Descrição
Vítima	Uma carga de trabalho definida pelo usuário cujo desempenho diminuiu devido a outras cargas de trabalho, chamadas de "valentões", que estão sobrecarregando um componente do cluster. Somente as cargas de trabalho definidas pelo usuário são identificadas como vítimas. O Unified Manager identifica as cargas de trabalho vítimas com base no desvio de latência, em que a latência real, durante um evento, aumentou significativamente em relação à latência prevista (faixa esperada).
Valentão	Uma carga de trabalho definida pelo usuário ou pelo sistema, cujo uso excessivo de um componente do cluster causou a queda de desempenho de outras cargas de trabalho, chamadas de vítimas. O Unified Manager identifica as cargas de trabalho problemáticas com base no desvio no uso de um componente do cluster, em que o uso real, durante um evento, aumentou significativamente em relação à faixa de uso esperada.
Tubarão	Uma carga de trabalho definida pelo usuário com o maior uso de um componente do cluster em comparação com todas as cargas de trabalho envolvidas em um evento. O Unified Manager identifica as cargas de trabalho shark com base no uso de um componente do cluster durante um evento.

As cargas de trabalho em um cluster podem compartilhar muitos dos componentes do cluster, como agregados e a CPU para rede e processamento de dados. Quando uma carga de trabalho, como um volume, aumenta o uso de um componente do cluster a ponto de o componente não conseguir atender com eficiência às demandas da carga de trabalho, o componente entra em contenção. A carga de trabalho que usa em excesso um componente do cluster é um agressor. As outras cargas de trabalho que compartilham esses componentes e cujo desempenho é afetado pelo agressor são as vítimas. A atividade de cargas de trabalho definidas pelo sistema, como deduplicação ou cópias Snapshot, também pode escalar para “bullying”.

Quando o Unified Manager detecta um evento, ele identifica todas as cargas de trabalho e os componentes do cluster envolvidos, incluindo as cargas de trabalho invasoras que causaram o evento, o componente do cluster que está em disputa e as cargas de trabalho vítimas cujo desempenho diminuiu devido ao aumento da atividade das cargas de trabalho invasoras.



Se o Unified Manager não conseguir identificar as cargas de trabalho agressoras, ele emitirá alertas apenas sobre as cargas de trabalho vítimas e o componente do cluster envolvido.

O Unified Manager consegue identificar cargas de trabalho que são vítimas de cargas de trabalho abusivas e também identificar quando essas mesmas cargas de trabalho se tornam abusivas. Uma carga de trabalho pode ser abusiva consigo 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 também sejam limitadas, incluindo ela mesma. Uma carga de trabalho que é abusiva ou vítima em um evento de desempenho em andamento pode mudar sua função ou deixar de participar do evento.

Gerenciar limites de desempenho

Gerencie os limites de desempenho no Active IQ Unified Manager

As políticas de limite de desempenho permitem determinar 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 definidos pelo usuário, pelo sistema e dinâmicos. Com limites de desempenho dinâmicos e definidos pelo sistema, o Unified Manager analisa a atividade da carga de trabalho para determinar o valor de limite apropriado. Com limites definidos pelo usuário, você pode definir os limites superiores de desempenho para diversos contadores de desempenho e para diversos objetos de armazenamento.



Os limites de desempenho definidos pelo sistema e os limites de desempenho dinâmicos são definidos pelo Unified Manager e não podem ser configurados. Se você estiver recebendo eventos desnecessários de qualquer política de limite de desempenho definida pelo sistema, poderá desativar políticas individuais na página Configuração de eventos.

Utilize políticas de limite de desempenho definidas pelo usuário no Active IQ Unified Manager

Você define políticas de limite de desempenho em objetos de armazenamento (por exemplo, em agregados e volumes) para que o administrador de storage receba um evento informando que o cluster está apresentando um problema de desempenho.

Você cria uma política de limite de desempenho para um objeto de storage da seguinte forma:

- Selecionando um objeto de armazenamento
- Selecionar um contador de desempenho associado a esse objeto
- Especificar valores que definem os limites superiores do contador de desempenho considerados situações de aviso e críticas
- Especificar um período de tempo que define por quanto tempo o contador deve exceder o limite superior

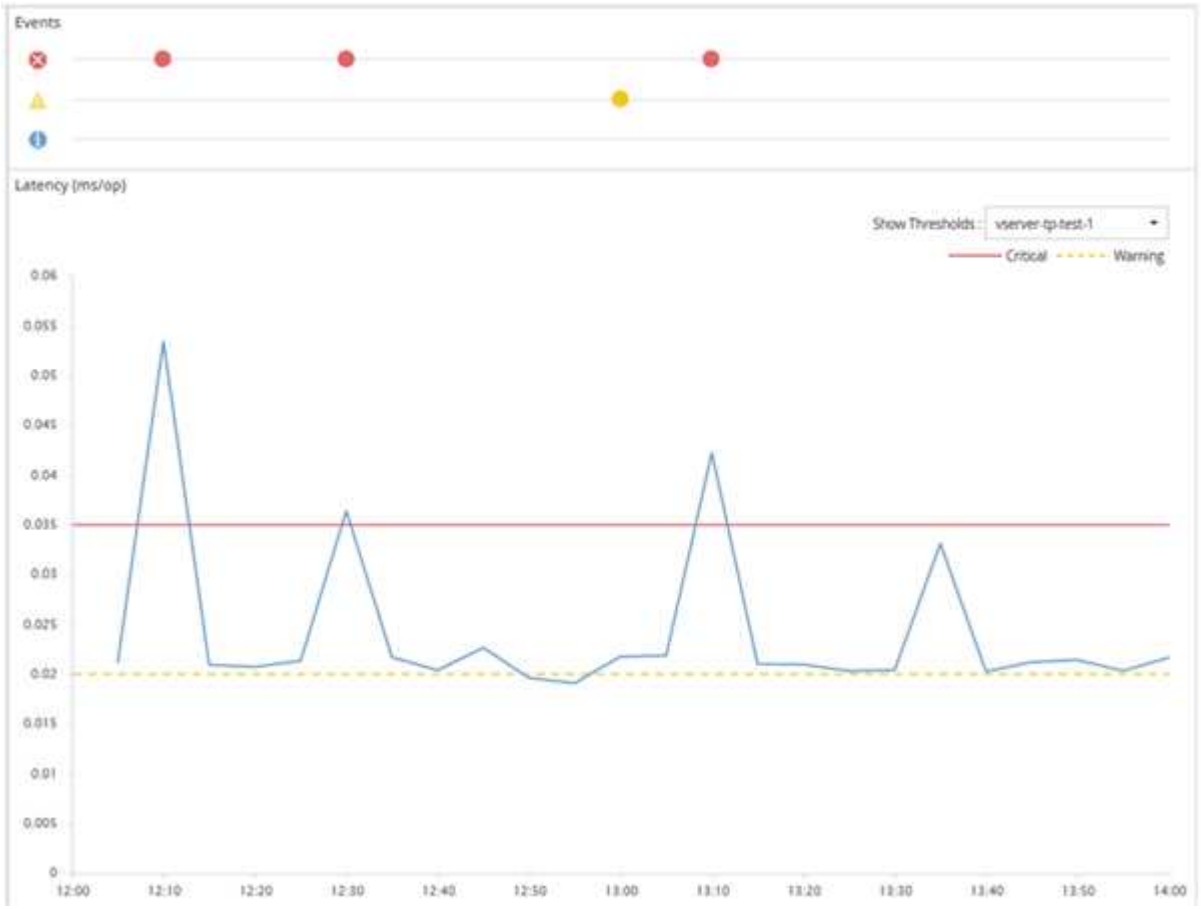
Por exemplo, você pode definir uma política de limite de desempenho em um volume para receber uma notificação de evento crítico sempre que o IOPS desse volume exceder 750 operações por segundo durante 10 minutos consecutivos. Essa mesma política de limite também pode especificar o envio de um evento de aviso quando o IOPS exceder 500 operações por segundo durante 10 minutos.



A versão atual oferece limites que enviam eventos quando o valor de um contador excede o limite definido. Não é possível definir limites que enviem eventos quando o valor de um

contador ficar abaixo do limite definido.

Aqui está um exemplo de gráfico de contadores, indicando que um limite de alerta (ícone amarelo) foi ultrapassado à 1:00 e que um limite crítico (ícone vermelho) foi ultrapassado às 12:10, 12:30 e 1:10:



Uma violação do 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 um novo período.

Alguns objetos de cluster e contadores de desempenho permitem criar uma política de limite combinada 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 do cluster	Contador de desempenho	Limiar de alerta	Limiar crítico	Duração
Volume	Latência	10 milissegundos	20 milissegundos	15 minutos
Agregado	Utilização	65%	85%	

Políticas de limite que usam dois objetos de cluster geram um evento somente quando ambas as condições são violadas. Por exemplo, usando a política de limite definida na tabela:

Se a latência do volume estiver em média…	E a utilização de disco do agregado é…	Então…
15 milissegundos	50%	Nenhum evento foi relatado.
15 milissegundos	75%	Um evento de aviso é relatado.

Se a latência do volume estiver em média…	E a utilização de disco do agregado é…	Então…
25 milissegundos	75%	Um evento de aviso é relatado.
25 milissegundos	90%	Um evento crítico foi relatado.

Responda às políticas de limite de desempenho violadas no Active IQ Unified Manager

Quando o valor de um contador excede o valor definido do limite de desempenho pelo período especificado na duração, o limite é violado e um evento é gerado.

O evento faz com que as seguintes ações sejam iniciadas:

- O evento é exibido no Dashboard, na página Performance Cluster Summary, na página Events e na página Performance Inventory específica do objeto.
- (opcional) é possível enviar um alerta por e-mail sobre o evento para um ou mais destinatários de e-mail, e um trap SNMP para um receptor de traps.
- (opcional) Um script pode ser executado para modificar ou atualizar automaticamente os objetos de armazenamento.

A primeira ação é sempre executada. Você configura se as ações opcionais serão realizadas na página de Configuração de Alertas. É possível definir ações específicas dependendo de uma política de limite de Aviso ou Crítico ser violada.

Após ocorrer uma violação da política de limite de desempenho em um objeto de storage, nenhum outro evento é 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 continuar a ser excedido, o horário de término do evento é atualizado continuamente para refletir que esse evento ainda está em andamento.

Um evento de limite captura, ou congela, as informações relacionadas à gravidade e à definição da política, de modo que as informações exclusivas do limite sejam exibidas com o evento, mesmo que a política de limite seja modificada no futuro.

Entenda os contadores de desempenho monitorados por meio de limites no Active IQ Unified Manager

Alguns contadores de desempenho comuns, como IOPS e MB/s, podem ter limites definidos para todos os objetos de armazenamento. Existem outros contadores que podem ter limites definidos apenas para determinados objetos de armazenamento.

Contadores de desempenho disponíveis

Objeto de armazenamento	Contador de desempenho	Descrição
Cluster	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

Objeto de armazenamento	Contador de desempenho	Descrição
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 da aplicação.
Utilização	Porcentagem média de uso da CPU e da RAM do nó.	Capacidade de desempenho utilizada
Percentual médio da capacidade de desempenho que o nó está consumindo.	Capacidade de desempenho utilizada - takeover	Percentual médio da capacidade de desempenho consumida pelo nó, mais a capacidade de desempenho do nó parceiro.
Agregado	IOPS	Número médio de operações de entrada/saída que o agregado processa 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	Percentual médio dos discos do agregado que estão sendo usados.
Capacidade de desempenho utilizada	Porcentagem média da capacidade de desempenho que está sendo consumida pelo agregado.	VM de armazenamento
IOPS	Número médio de operações de entrada/saída processadas pela SVM por segundo.	MB/s
Número médio de megabytes de dados transferidos de e para esta SVM por segundo.	Latência	Número médio de milissegundos que a SVM leva para responder às solicitações da aplicação.
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 da aplicação.	Taxa de falhas 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.

Objeto de armazenamento	Contador de desempenho	Descrição
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 da aplicação.	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 da largura de banda	Porcentagem média da largura de banda disponível da porta que está sendo utilizada.	MB/s
Número médio de megabytes de dados transferidos de e para esta porta por segundo.	Interface de Rede (LIF)	MB/s

Compreenda os objetos de política de limite combinado e os contadores no Active IQ Unified Manager

Apenas alguns contadores de desempenho podem ser usados em conjunto em políticas combinadas. Quando contadores de desempenho primários e secundários são especificados, ambos os contadores de desempenho devem exceder seus limites máximos para gerar um evento.

Objeto de armazenamento primário e contador	Objeto de armazenamento secundário e contador
Latência de volume	IOPS do volume
MB/s do volume	Utilização do agregado
Capacidade de desempenho agregada utilizada	Utilização de nós
Capacidade de desempenho do nó utilizada	Capacidade de desempenho do nó usada: tomada de controle
Latência da LUN	IOPS do LUN
MB/s do LUN	Utilização do agregado
Capacidade de desempenho agregada utilizada	Utilização de nós
Capacidade de desempenho do nó utilizada	Capacidade de desempenho do nó usada: tomada de controle

Quando uma política de combinação de volumes é aplicada a um volume FlexGroup, em vez de a um volume FlexVol, somente os atributos “IOPS do volume” e “MB/s do volume” podem ser selecionados como 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 no Active IQ Unified Manager

Você cria políticas de limite de desempenho para objetos de armazenamento para que as notificações sejam enviadas quando um contador de desempenho exceder um valor específico. A notificação de evento identifica que o cluster está apresentando um problema de desempenho.

Antes de começar

Você precisa ter a função de Application Administrator.

Você cria políticas de limite de desempenho inserindo os valores de limite na página Criar Política de Limite de Desempenho. Você pode criar novas políticas definindo todos os valores da política nesta página ou pode fazer uma cópia de uma política existente e alterar os valores na cópia (processo chamado de *clonagem*).

Os valores limite válidos são de 0,001 a 10.000.000 para números, de 0,001 a 100 para porcentagens e de 0,001 a 200 para porcentagens de capacidade de desempenho usada.

A versão atual oferece limites que enviam eventos quando o valor de um contador excede o limite definido. Não é possível definir limites que enviem eventos quando o valor de um contador ficar abaixo do limite definido.

Passos

1. No painel de navegação esquerdo, selecione **Limiares de eventos** > **Desempenho**.

   A página Limites de desempenho é exibida.

2. Clique no botão apropriado, dependendo de você querer criar uma nova política ou 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 Create Performance Threshold Policy ou a página Clone Performance Threshold Policy 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 que você quer monitorar e especifique os valores limite que definem os eventos de aviso e crítico.

      Você deve definir pelo menos um limite de aviso ou um limite crítico. Não é necessário definir os dois tipos de limite.

c. Selecione um contador de desempenho secundário, se necessário, e especifique os valores limite para eventos de aviso e críticos.

   A inclusão de um contador secundário exige que ambos os contadores excedam os valores limite antes que o limite seja ultrapassado e um evento seja reportado. Somente determinados objetos e contadores podem ser configurados usando uma política combinada.

d. Selecione o período de tempo durante o qual os valores limite devem ser ultrapassados para que um evento seja enviado.

Ao clonar uma política existente, você deve inserir um novo nome para a política.

4. Clique em **Salvar** para salvar a política.

   Você retorna à página Limiares de Desempenho. Uma mensagem de sucesso na parte superior da página confirma que a política de limiar foi criada e fornece um link para a página de Inventário desse 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 até a página Inventário.

Atribua políticas de limite de desempenho a objetos de storage no Active IQ Unified Manager

Você atribui uma política de limite de desempenho definida pelo usuário a um objeto de armazenamento para que o Unified Manager registre um evento se o valor do contador de desempenho exceder a configuração da política.

Antes de começar

Você precisa ter a função de Application Administrator.

A política ou as 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 ainda não atingiram seu valor máximo
- Ignora os objetos que já atingiram o número máximo de políticas
- Exibe uma mensagem informando que a política não foi atribuída a todos os objetos

Passos

1. Na página de inventário de desempenho de qualquer objeto de armazenamento, selecione o objeto ou os 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.

Para atribuir limites a…	Clique…
Todos os objetos na página	Na caixa suspensa , escolha **Selecionar todos os objetos desta página**.
Todos os objetos do mesmo tipo	Na caixa suspensa, escolha **Selecionar todos os objetos**.

Você pode usar a funcionalidade de classificação e filtragem para refinar a lista de objetos na página de inventário, facilitando a aplicação de políticas de limite a vários objetos.

2. Faça sua seleção e, em seguida, clique em **Atribuir Política de Limite de Desempenho**.

   A página "Atribuir Política de Limite de Desempenho" é exibida e mostra uma lista das 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 e verificar se você selecionou a política de limite correta.
4. Após selecionar a política de limite apropriada, clique em **Atribuir Política**.

   Uma mensagem de sucesso na parte superior da página confirma que a política de limite foi atribuída ao objeto ou aos objetos e fornece um link para a página de alertas para que você possa configurar as configurações de alerta para este objeto e esta política.

Se você quiser que os alertas sejam enviados por e-mail ou como um trap SNMP para notificar você de que um determinado evento de desempenho foi gerado, você deve configurar as definições de alerta na página Alert Setup.

Visualize as políticas de limite de desempenho no Active IQ Unified Manager

Você pode visualizar todas as políticas de limite de desempenho definidas atualmente na página Performance Thresholds.

A lista de políticas de limite é classificada em ordem alfabética pelo nome da política e inclui políticas para todos os tipos de objetos de armazenamento. Você pode clicar no cabeçalho de uma coluna para classificar as políticas por essa coluna. Se você estiver procurando uma política específica, use os mecanismos de filtro e pesquisa para refinar a lista de políticas de limite que aparecem na lista de inventário.

Você pode passar o cursor sobre o Nome da Política e o nome da Condição para ver os detalhes de configuração da política. Além disso, você pode usar os botões fornecidos para criar, clonar, editar e excluir políticas de limite definidas pelo usuário.

Etapa

1. No painel de navegação esquerdo, selecione **Limiares de eventos** > **Desempenho**.

   A página Limites de desempenho é exibida.

Edite as políticas de limite de desempenho definidas pelo usuário no Active IQ Unified Manager

Você pode editar as configurações de limite para políticas de limite de desempenho existentes. Isso pode ser útil se você perceber que está recebendo alertas em excesso ou em falta para determinadas condições de limite.

Antes de começar

Você precisa ter a função de Application Administrator.

Não é possível alterar o nome da política nem o tipo de objeto de armazenamento monitorado para as políticas de limite existentes.

Passos

1. No painel de navegação esquerdo, selecione **Limiares de eventos** > **Desempenho**.

   A página Limiares de Desempenho é exibida.

2. Selecione a política de limite que deseja alterar e clique em **Editar**.

   A página Editar política de limite de desempenho é exibida.

3. Faça as alterações desejadas na política de limite e clique em **Salvar**.

   Você volta para a página Limiares de desempenho.

Depois que você as salva, as alterações são aplicadas imediatamente a todos os objetos de armazenamento que usam a política.

Dependendo do tipo de alterações que você fez na política, talvez seja necessário revisar as configurações de alerta definidas para os objetos que usam a política na página Configuração de Alertas.

Remova as políticas de limite de desempenho dos objetos de armazenamento no Active IQ Unified Manager

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 precisa ter a função de Application Administrator.

Você só pode remover 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 de **inventário** de qualquer objeto de armazenamento, selecione um ou mais objetos que tenham pelo menos uma política de limite de desempenho aplicada.

Para limpar os limiares 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 em ☐▾ no cabeçalho da coluna.

2. Clique em **Clear Performance Threshold Policy**.

   A página Clear Threshold Policy é exibida, mostrando uma lista de políticas de limite atribuídas atualmente aos objetos de armazenamento.

3. Selecione a política de limite que deseja remover dos objetos e clique em **Clear Policy**.

   Ao selecionar uma política de limite, os detalhes da política são exibidos para que você possa confirmar se selecionou a política apropriada.

Entenda as alterações nas políticas de limite de desempenho no Active IQ Unified Manager

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 storage que usam a política. A nova configuração entra em vigor imediatamente, e o Unified Manager começa a comparar os valores do contador de desempenho com as novas configurações de limite para todos os dados de desempenho recém-coletados.

Se existirem eventos ativos para objetos que estejam usando a política de limite alterada, os eventos serão marcados como obsoletos e a política de limite começará a monitorar o contador como uma política de limite recém-definida.

Ao visualizar o contador ao qual o limite foi aplicado na Visualização Detalhada dos Gráficos de Contadores, 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 Visualização detalhada dos gráficos do contador, você poderá ver eventos históricos que parecem estar abaixo das linhas de limite atuais.

Gerencie políticas de limite ao mover objetos no Active IQ Unified Manager

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 vinculadas 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 secundária para a política de limite (uma política combinada), por exemplo, se uma condição adicional for atribuída a um agregado ou a um nó, a condição de contador secundária 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, esses 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 ONTAP envie um evento de alteração informativo. Um ícone de evento de alteração aparece na linha do tempo de Eventos na página Performance Explorer e na página Workload Analysis para indicar o momento em que a operação de movimentação foi concluída.

Ao mover um objeto para um cluster diferente, a política de limite definida pelo usuário é removida do objeto. Caso necessário, você deve atribuir uma política de limite ao objeto após a conclusão da operação de movimentação. Políticas de limite dinâmicas e definidas pelo sistema, no entanto, são aplicadas automaticamente a um objeto após ele ser movido para um novo cluster.

Funcionalidade da política de limite durante o takeover de HA e o giveback

Quando ocorre uma operação de takeover ou giveback em uma configuração de alta disponibilidade (HA), os objetos movidos de um nó para o outro mantêm suas políticas de limite da mesma forma que nas operações de movimentação manual. Como o Unified Manager verifica as alterações na configuração do cluster a cada 15 minutos, o impacto do switchover para o novo nó só é identificado na próxima verificação da configuração do cluster.

Se uma operação de takeover e uma de giveback ocorrerem 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 da política de limiar durante a realocação de agregado

Se você mover um agregado de um nó para outro usando o `aggregate relocation start` comando, as políticas de limite individuais e combinadas são mantidas em todos os objetos, e a parte da política de limite referente ao nó é aplicada ao novo nó.

Funcionalidade da política de limite durante o switchover do MetroCluster

Os objetos que são movidos de um cluster para outro em uma configuração do MetroCluster não mantêm suas configurações de política de limite definidas pelo usuário. Se necessário, você pode aplicar políticas de limite aos volumes e LUNs que foram movidos para o cluster parceiro. Depois que um objeto retorna ao seu cluster original, a política de limite definida pelo usuário é reaplicada automaticamente.

Para informações, consulte "Comportamento do volume durante switchover e switchback".

Analisar eventos de desempenho

Analise eventos de desempenho no Active IQ Unified Manager

Você pode analisar eventos de desempenho para identificar quando foram detectados, se estão ativos (novos ou reconhecidos) ou obsoletos, as cargas de trabalho e os componentes do cluster envolvidos, bem como as opções para resolver os eventos por conta própria.

Exibir informações sobre eventos de desempenho no Active IQ Unified Manager

Você pode usar a página de inventário do Event Management 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, detalhar as informações para determinar a causa do evento.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

A lista de eventos é ordenada por horário de detecção, com os eventos mais recentes listados primeiro. Você pode clicar no cabeçalho de uma coluna para ordenar os eventos com base nessa coluna. Por exemplo, você pode ordenar pela coluna Status para visualizar os eventos por gravidade. Se você estiver procurando um evento específico ou um tipo específico de evento, poderá usar os mecanismos de filtro e pesquisa para refinar a lista de eventos exibidos 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
- Limiar de desempenho dinâmico

A coluna Tipo de Evento lista a origem do evento. Você pode selecionar um evento para ver detalhes sobre o evento na página de detalhes do evento.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.
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 o evento que você deseja analisar e clique no nome do evento.

   A página com os 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 Explorador de Desempenho e em um e-mail de alerta.

Analisar eventos a partir de limites de desempenho definidos pelo usuário

Analise eventos a partir de limites de desempenho definidos pelo usuário no Active IQ Unified Manager

Os 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 do cluster está apresentando um problema de desempenho.

Você usa a página Detalhes do evento para analisar o evento de desempenho e tomar medidas corretivas, se necessário, para fazer o desempenho voltar ao normal.

Responda a eventos de limite de desempenho definidos pelo usuário no Active IQ Unified Manager

Você pode usar o Unified Manager para investigar eventos de desempenho causados por um contador de desempenho que ultrapassou um limite de aviso ou crítico 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Deve haver eventos de desempenho novos ou obsoletos.

Passos

1. Exiba a página **Detalhes do evento** para visualizar informações sobre o evento.
2. Analise 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 WARNING 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 avaliado, o valor do contador que deve ser ultrapassado para ser considerado um evento crítico ou de aviso e a duração durante a qual o contador deve exceder esse valor.

4. Anote o **Horário de Disparo do Evento** para que você possa investigar se outros eventos podem ter ocorrido ao mesmo tempo e contribuído para este evento.
5. Siga uma das opções abaixo para investigar melhor o evento e determinar se é necessário realizar alguma ação para resolver o problema de desempenho:

Opção	Possíveis ações de investigação
Clique no nome do objeto de origem para exibir a página Explorer desse objeto.	Esta página permite visualizar os detalhes do objeto e compará-lo com outros objetos de armazenamento semelhantes para verificar se outros objetos de armazenamento apresentam problemas de desempenho no mesmo período. Por exemplo, para verificar se outros volumes no mesmo agregado também estão apresentando 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 verificar se outros problemas de desempenho ocorreram aproximadamente ao mesmo tempo.

Analisar eventos a partir de limites de desempenho definidos pelo sistema

Analise eventos a partir de limites de desempenho definidos pelo sistema no Active IQ Unified Manager

Os 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 estabelecido por uma política do sistema. Isso indica que o objeto de armazenamento, por exemplo, um agregado ou nó, está apresentando um problema de desempenho.

Você usa a página Detalhes do evento para analisar o evento de desempenho e tomar medidas corretivas, se necessário, para fazer o desempenho voltar ao normal.

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

Responda a eventos de limite de desempenho definidos pelo sistema no Active IQ Unified Manager

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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Deve haver eventos de desempenho novos ou obsoletos.

Passos

1. Exiba a página **Detalhes do evento** para visualizar informações sobre o evento.
2. Analise 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 WARNING 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 Disparo do Evento** para que você possa investigar se outros eventos podem ter ocorrido ao mesmo tempo e contribuído para este evento.
4. Em **Diagnóstico do Sistema**, revise a breve descrição do tipo de análise que a política definida pelo sistema está realizando 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, gráficos de contadores 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 no Active IQ Unified Manager

O Unified Manager gera eventos de aviso de política de QoS quando a taxa de transferência da carga de trabalho (IOPS, IOPS/TB ou MBps) excede a configuração definida da política de QoS do ONTAP e a latência da carga de trabalho começa a ser 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

- Devem existir eventos de desempenho novos, reconhecidos ou obsoletos.

O Unified Manager gera eventos de alerta para violações da política de QoS quando a taxa de transferência da carga de trabalho excede a configuração definida da política de QoS durante cada período de coleta de desempenho da hora anterior. A taxa de transferência da carga de trabalho pode exceder o limite de QoS apenas por um curto período 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 talvez não tenha ultrapassado o limite da política exibido no gráfico.

Você pode usar o System Manager ou os comandos do 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
- Transferir 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. Analise a **Descrição**, que descreve a violação do limite que causou o evento.

   Por exemplo, a mensagem “O valor de IOPS de 1,352 IOPS em vol1_NFS1 acionou um evento WARNING para identificar possíveis problemas de desempenho da carga de trabalho” indica que ocorreu um evento QoS Max IOPS no volume vol1_NFS1.

3. Consulte a seção **Event Information** para obter mais detalhes sobre quando o evento ocorreu e por 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 consomem mais IOPS ou MBps.

4. Na seção **System Diagnosis**, revise os dois gráficos: um para a média total de IOPS ou MBps (dependendo do evento) e outro para a latência. Dessa forma, você poderá ver quais componentes do cluster estão afetando mais a latência quando a carga de trabalho se aproximou do limite máximo de QoS.

   Para um evento de política de QoS compartilhada, as três principais cargas de trabalho são exibidas no gráfico de throughput. Se mais de três cargas de trabalho compartilharem a política de QoS, as cargas de trabalho adicionais serão agrupadas em uma categoria "Outras cargas de trabalho". Além disso, o gráfico de latência mostra a latência média de 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 **Help** para ver mais detalhes sobre as ações sugeridas que você pode executar para tentar resolver o evento de desempenho.

Entenda os eventos de QoS adaptável com um tamanho de bloco definido no Active IQ Unified Manager

Os grupos de políticas de QoS adaptáveis dimensionam automaticamente um limite máximo ou mínimo de taxa de transferência com base no tamanho do volume, mantendo a proporção de IOPS para TBs à medida que 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 simultaneamente.

Atribuir um limite de IOPS em uma política de QoS adaptável limita apenas o número de operações que ocorrem em cada carga de trabalho. Dependendo do tamanho do bloco definido no cliente que gera as cargas de trabalho, algumas IOPS incluem muito mais dados e, portanto, impõem uma carga muito maior aos nós que processam as operações.

O valor em MB/s para uma carga de trabalho é gerado usando a seguinte fórmula:

```
MB/s = (IOPS * 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, a taxa de transferência efetiva (MB/s) para essa carga de trabalho será de 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, a taxa de transferência efetiva (MB/s) para essa carga de trabalho será de 144. É possível observar que o nó processa 50% mais dados quando o tamanho do bloco é maior.

Vamos analisar 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 configurado no cliente.

Crie uma política e defina o limite de taxa de transferência para 2.500 IOPS/TB com um tamanho de bloco de 32 KB. Isso define efetivamente o limite de MB/s como 80 MB/s ((2.500 IOPS * 32 KB) / 1.000) para um volume com 1 TB de capacidade usada. Observe que o Unified Manager gera um evento de aviso quando o valor da taxa de transferência é 10% menor 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, e o IOPS for 4.000, e o tamanho do bloco de QoS estiver definido como 32 KB no cliente, então a taxa de transferência em MB/ps será de 128 MB/s ((4.000 IOPS * 32 KB) / 1000). Nenhum evento é gerado neste cenário porque tanto 4.000 IOPS quanto 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, e o IOPS for 4.000, e o tamanho do bloco de QoS estiver definido como 64 KB no cliente, então a taxa de transferência em MB/s será de 256 MB/s ((4.000 IOPS * 64 KB) / 1000). Nesse caso, os 4.000 IOPS não geram um evento, mas o valor de 256 MB/s está acima do limite de 144 MB/s e gera um evento.

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 System Diagnosis da página Event details. Se o evento for acionado com base em uma violação de IOPS para a política de QoS adaptável, um gráfico de IOPS é exibido na seção System Diagnosis. Se ocorrer uma violação tanto de IOPS quanto de MB/s, você receberá dois eventos.

Para obter mais informações sobre como ajustar as configurações de QoS, consulte "Visão geral do gerenciamento de desempenho".

Responder a eventos de sobreutilização de recursos de nós no Active IQ Unified Manager

O Unified Manager gera eventos de aviso de sobrecarga de recursos de nós quando um único nó está operando acima dos limites de sua eficiência operacional e, portanto, potencialmente afetando as latências das cargas 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Deve haver eventos de desempenho novos ou obsoletos.

O Unified Manager gera eventos de alerta para violações de política de sobreutilização de recursos de nó ao procurar nós que estejam utilizando mais de 100% de sua capacidade de desempenho por mais de 30 minutos.

Você pode usar o System Manager ou os comandos do 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
- Redução do 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. Analise a **Descrição**, que descreve a violação do limite que causou o evento.

   Por exemplo, a mensagem “Perf. O valor de 139% de Capacity Used em simplicity-02 acionou um evento de WARNING 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 a capacidade de desempenho utilizada no nó, um para a média de IOPS de armazenamento utilizada pelas principais cargas de trabalho e um para a latência nas principais cargas de trabalho. Ao organizá-los dessa forma, você poderá identificar 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 têm, 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 **Help** 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 no Active IQ Unified Manager

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 das cargas 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

O Unified Manager gera eventos de alerta para violações da política de limite de desequilíbrio do cluster, comparando o valor da capacidade de desempenho usada em todos os nós do cluster para verificar se há uma diferença de carga de 30% entre quaisquer nós.

Estas etapas ajudam você a identificar os seguintes recursos para que possa mover cargas de trabalho de alto desempenho para um nó menos utilizado:

- Os nós do mesmo cluster que estão menos utilizados
- Os agregados no novo nó que são menos utilizados
- Os volumes de melhor desempenho no nó atual

Passos

1. Exiba a página de detalhes do **Event** para visualizar informações sobre o evento.
2. Analise 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 do cluster Dallas-1-8 e acionou um evento de AVISO com base no limite do sistema de 30%” indica que a capacidade de desempenho em um dos nós está sobreutilizada e afetando o desempenho do nó.

3. Analise o texto em **Ações Sugeridas** para mover um volume de alto desempenho do nó com o maior valor de capacidade de desempenho utilizada para um nó com o menor valor de capacidade de desempenho utilizada.
4. Identifique os nós com o maior e o menor valor de capacidade de desempenho utilizada:
   a. Na seção **Informações do evento**, clique no nome do cluster de origem.
   b. Na página **Resumo do Cluster / Desempenho**, clique em **Nós** na área **Objetos Gerenciados**.
   c. Na página de inventário **Nós**, classifique os nós pela coluna **Capacidade de Desempenho Utilizada**.
   d. Identifique os nós com o maior e o menor valor de capacidade de desempenho usado e anote esses nomes.
5. Identifique o volume que usa mais IOPS no nó com o maior valor de capacidade de desempenho utilizada:

a. Clique no nó com o maior valor de capacidade de desempenho usada.
b. Na página **Node / Performance Explorer**, selecione **Aggregates on this Node** no menu **View and Compare**.
c. Clique no agregado com o maior valor de capacidade de desempenho utilizada.
d. Na página **Aggregate / Performance Explorer**, selecione **Volumes on this Aggregate** no menu **View and Compare**.
e. Ordene os volumes pela coluna **IOPS** e anote o nome do volume que usa mais IOPS e o nome do agregado onde o volume reside.

6. Identifique o agregado com a menor utilização no nó que apresenta o menor valor de capacidade de desempenho utilizada:
   a. Clique em **Storage** > **Aggregates** para exibir a página de inventário de **Aggregates**.
   b. Selecione a visualização **Desempenho: todos os agregados**.
   c. Clique no botão **Filter** e adicione um filtro em que “Node” seja igual ao nome do nó com o menor valor de capacidade de desempenho usada que você anotou na etapa 4.
   d. Anote o nome do agregado que possui 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, comandos do 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 dinâmicos

Analise eventos a partir de limites de desempenho dinâmicos no Active IQ Unified Manager

Os eventos gerados a partir de limites dinâmicos indicam que o tempo de resposta (latência) real de uma carga de trabalho está muito alto ou muito baixo em comparação com a faixa de tempo de resposta esperada. Você usa a página Detalhes do evento para analisar o evento de desempenho e tomar medidas corretivas, se necessário, para restaurar o desempenho ao normal.

Os limites de desempenho dinâmicos não estão habilitados nos sistemas Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select.

Identifique cargas de trabalho afetadas em eventos de desempenho dinâmicos no Active IQ Unified Manager

No Unified Manager, você pode identificar quais cargas de trabalho de volume apresentam o maior desvio no tempo de resposta (latência) causado por um componente de armazenamento em disputa. Identificar essas cargas de trabalho ajuda você a entender por que os aplicativos cliente que acessam esses volumes estão apresentando desempenho mais lento do que o normal.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Deve haver eventos de desempenho dinâmico novos, reconhecidos ou obsoletos.

A página de detalhes do evento exibe uma lista das cargas de trabalho definidas pelo usuário e pelo sistema, classificadas pelo maior desvio na atividade ou no uso do componente ou pelo maior impacto causado 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 vítimas**.
3. Passe o cursor sobre os gráficos para visualizar as principais cargas de trabalho definidas pelo usuário que estão afetando o componente, bem como o nome da carga de trabalho vítima.

Identifique cargas de trabalho excessivas em eventos de desempenho dinâmicos no Active IQ Unified Manager

No Unified Manager, você pode identificar quais cargas de trabalho têm o maior desvio de uso em um componente do cluster em contenção. Identificar essas cargas de trabalho ajuda você a entender por que determinados volumes no cluster têm tempos de resposta lentos (latência).

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Deve haver eventos de desempenho dinâmico novos, reconhecidos ou obsoletos.

A página de detalhes do evento exibe uma lista das cargas de trabalho definidas pelo usuário e pelo sistema, classificadas pelo maior uso do componente ou pelo maior impacto causado 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 de detalhes do evento para visualizar informações sobre o evento.
2. Nos gráficos de latência da carga de trabalho e atividade da carga de trabalho, selecione **Bully Workloads**.
3. Passe o cursor sobre os gráficos para visualizar as principais cargas de trabalho agressoras definidas pelo usuário que estão afetando o componente.

Identifique cargas de trabalho shark em um evento de desempenho dinâmico no Active IQ Unified Manager

No Unified Manager, você pode identificar quais cargas de trabalho apresentam o maior desvio de uso de um componente de armazenamento em contenção. Identificar essas cargas de trabalho ajuda você a determinar se elas devem ser movidas para um cluster menos utilizado.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Há um evento dinâmico de desempenho novo, reconhecido ou obsoleto.

A página de detalhes do evento exibe uma lista das cargas de trabalho definidas pelo usuário e pelo sistema, classificadas pelo maior uso do componente ou pelo maior impacto causado 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 de Latência da carga de trabalho e Atividade da carga de trabalho, selecione **Shark Workloads**.
3. Posicione o cursor sobre os gráficos para ver as principais cargas de trabalho definidas pelo usuário que estão afetando o componente, bem como o nome da carga de trabalho shark.

Análise de eventos de desempenho para uma configuração do MetroCluster

Analise o MetroCluster eventos de desempenho com o Active IQ Unified Manager

Você pode usar o Unified Manager para analisar um evento de desempenho de 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 causados por cargas de trabalho "bully" que estão sobreutilizando os links entre switches (ISLs) entre os clusters ou por problemas de integridade dos links. O Unified Manager monitora cada cluster em uma configuração do MetroCluster de forma independente, sem considerar os eventos de desempenho em um cluster parceiro.

Os eventos de desempenho de ambos os clusters na configuração do MetroCluster também são exibidos na página Dashboard do Unified Manager. Você também pode visualizar as páginas de integridade do Unified Manager para verificar a integridade de cada cluster e visualizar o relacionamento entre eles.

Analise um evento de desempenho do MetroCluster em um cluster no Active IQ Unified Manager

Você pode usar o Unified Manager para analisar o cluster em uma configuração do MetroCluster na qual foi detectado um evento de desempenho. Você pode identificar o nome do cluster, o horário de detecção do evento e as cargas de trabalho *agressora* e *vítima* envolvidas.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Deve haver eventos de desempenho novos, reconhecidos ou obsoletos para uma configuração MetroCluster.
- Ambos os clusters na configuração do MetroCluster devem ser monitorados pela mesma instância do Unified Manager.

Passos

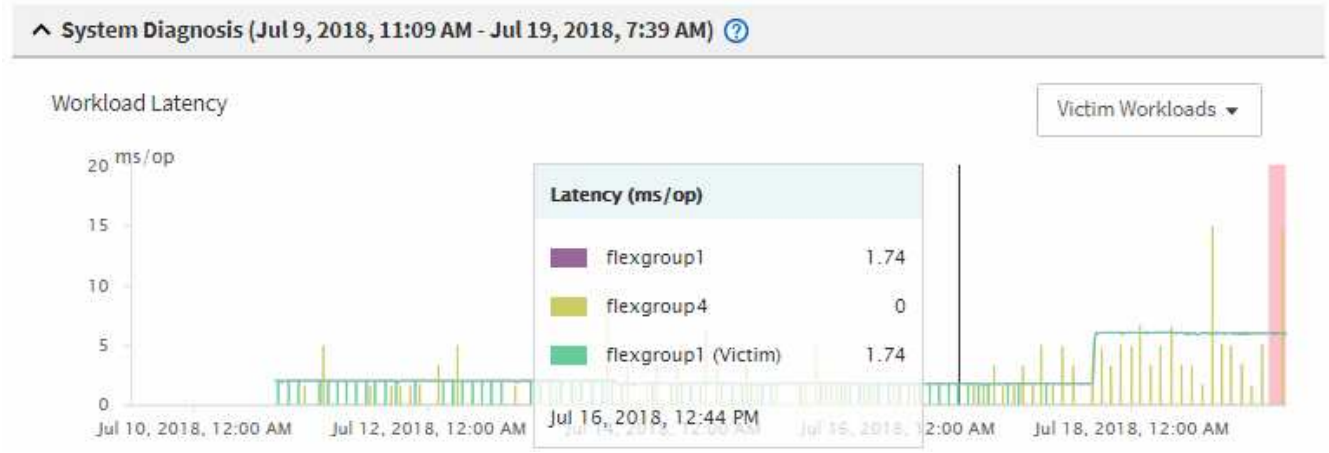
1. Exiba a página **Detalhes do evento** para visualizar informações sobre o evento.
2. Analise a descrição do evento para ver os nomes das cargas de trabalho envolvidas e o número de cargas de trabalho envolvidas.

   Neste exemplo, o ícone de Recursos do MetroCluster está vermelho, indicando que os recursos do MetroCluster estão em disputa. Você posiciona 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 poderá usar para analisar eventos de desempenho no cluster parceiro.
4. Nos gráficos, analise as cargas de trabalho da *vítima* para confirmar se seus tempos de resposta são superiores ao limite de desempenho.

   Neste exemplo, a carga de trabalho vítima é exibida no texto ao passar o cursor. Os gráficos de latência mostram, em alto nível, um padrão de latência consistente para as cargas de trabalho vítimas envolvidas. Embora a latência anormal das cargas de trabalho vítimas tenha acionado o evento, um padrão de latência consistente pode indicar que as cargas de trabalho estão operando dentro da faixa esperada, mas que um pico de E/S aumentou a latência e acionou o evento.



   Se você instalou recentemente um aplicativo em um cliente que acessa essas cargas de trabalho de volume e esse aplicativo envia uma grande quantidade de E/S para elas, você pode prever que a latência delas aumente. Se a latência das cargas de trabalho voltar 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 continuar e permanecer no novo estado, você poderá investigá-lo mais a fundo para determinar se outros problemas causaram o evento.

5. No gráfico Taxa de transferência da carga de trabalho, selecione **Cargas de trabalho agressoras** para exibir as cargas de trabalho agressoras.

   A presença de cargas de trabalho excessivas indica que o evento pode ter sido causado por uma ou mais cargas de trabalho no cluster local que sobrecarregaram os recursos do MetroCluster. As cargas de trabalho excessivas apresentam um desvio elevado na taxa de transferência de gravação (MB/s).

   Este gráfico exibe, em alto nível, o padrão da taxa de transferência de gravação (MB/s) para as cargas de trabalho. Você pode analisar o padrão de MB/s de gravação para identificar taxas de transferência anormais, que podem indicar que uma carga de trabalho está sobrecarregando os recursos do MetroCluster.

   Se não houver cargas de trabalho excessivas envolvidas no evento, ele pode ter sido causado por um problema de integridade no link entre os clusters ou por um problema de desempenho no cluster parceiro.

Você pode usar o Unified Manager para verificar a integridade de ambos os clusters em uma configuração de MetroCluster. Você também pode usar o Unified Manager para verificar e analisar eventos de desempenho no cluster parceiro.

Analise um evento de desempenho do MetroCluster em um cluster remoto no Active IQ Unified Manager

Você pode usar o Unified Manager para analisar eventos de desempenho dinâmico em um cluster remoto em uma configuração MetroCluster. A análise ajuda você a determinar se um evento no cluster remoto causou um evento no cluster parceiro.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Você deve ter analisado um evento de desempenho em um cluster local em uma configuração do MetroCluster e obtido o horário de detecção do evento.
- Você deve ter verificado a integridade do cluster local e do cluster parceiro envolvido no evento de desempenho, além de ter obtido o nome do cluster parceiro.

Passos

1. Faça login na instância do Unified Manager que está monitorando o cluster parceiro.
2. No painel de navegação à esquerda, clique em **Eventos** para exibir a lista de eventos.
3. No seletor **Intervalo de tempo**, selecione **Última hora** e, em seguida, 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 período em que o evento foi detectado em seu parceiro.

5. Se o cluster selecionado tiver eventos detectados na última hora, compare o horário de detecção do evento com o horário de detecção do evento no cluster local.

   Se esses eventos envolverem cargas de trabalho agressoras causando contenção no componente de processamento de dados, uma ou mais dessas cargas agressoras podem ter causado o evento no cluster local. Você pode clicar no evento para analisá-lo e revisar as ações sugeridas para resolvê-lo na página de detalhes do evento.

   Se esses eventos não envolverem cargas de trabalho excessivas, eles não causaram o evento de desempenho no cluster local.

Responder a um evento de limitação dinâmica de QoS no Active IQ Unified Manager

Você pode usar o Unified Manager para investigar um evento de desempenho causado por um grupo de políticas de Quality of Service (QoS) que limita a taxa de transferência de cargas de trabalho (MB/s). Essa 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

- Devem existir eventos de desempenho novos, reconhecidos ou obsoletos.

Passos

1. Exiba a página **Detalhes do evento** para visualizar informações sobre o evento.
2. Leia **Description**, que exibe o nome das cargas de trabalho afetadas pela limitação.

   A descrição pode exibir a mesma carga de trabalho para a vítima e para o agressor, porque a limitação de recursos faz com que a carga de trabalho se torne vítima de si mesma.

3. Anote 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 de Latência da Carga de Trabalho e Utilização da Carga de Trabalho, selecione **Bully Workloads**.
5. Posicione 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 apresentou o maior desvio e fez com que a limitação ocorresse. A atividade representa a porcentagem do limite do grupo de políticas utilizada por cada carga de trabalho.

6. Na área **Suggested Actions**, clique no botão **Analyze Workload** da carga de trabalho principal.
7. Na página Workload Analysis, configure o gráfico Latency para exibir todos os Cluster Components e o gráfico Throughput para exibir Breakdown.

   Os gráficos de detalhamento são exibidos abaixo do gráfico de latência e do gráfico de IOPS.

8. Compare os limites de QoS no gráfico de **Latência** para ver qual nível de limitação afetou 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/s), 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/s, o que fez com que o grupo de políticas reduzisse sua atividade para 1.000 op/s.

9. Compare os valores de **latência de leitura/gravação** com os valores de **leitura/gravação/outros**.

   Ambos os gráficos mostram um grande 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 você a determinar se há uma alta taxa de transferência ou um grande número de operações que aumentou a latência. Você pode usar esses valores ao decidir aplicar um limite de grupo de políticas à taxa de transferência ou às operações.

10. Use o ONTAP System Manager para aumentar o limite atual do grupo de políticas para 1.300 op/sec.
11. Após um dia, retorne ao Unified Manager e insira a carga de trabalho que você registrou na Etapa 3 na página **Workload Analysis**.
12. Selecione o gráfico de detalhamento da taxa de transferência.

    O gráfico Leituras/Gravações/Outros é exibido.

13. Na parte superior da página, posicione o cursor sobre o ícone de evento de alteração ( ) para a alteração do limite do grupo de políticas.

14. Compare o gráfico de **Reads/writes/other** com o gráfico de **Latency**.

    As solicitações de leitura e gravação são as mesmas, mas a limitação parou e a latência diminuiu.

Responder a um evento de desempenho causado por falha de disco no Active IQ Unified Manager

Você pode usar o Unified Manager para investigar um evento de desempenho causado por cargas de trabalho que sobrecarregam 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Devem existir eventos de desempenho 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 afetados cuja latência foi afetada pelo componente do cluster em disputa. O agregado, que está no meio de uma reconstrução de RAID para substituir o disco com falha por um disco sobressalente, é o componente do cluster em disputa. Em Componente em Disputa, o ícone Aggregate é destacado em vermelho, e o nome do agregado é exibido entre parênteses.

3. No gráfico Workload Utilization, selecione **Bully Workloads**.
4. Passe o cursor sobre o gráfico para ver as principais cargas de trabalho agressoras que estão afetando o componente.

    As principais cargas de trabalho com o 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 de RAID. Uma reconstrução é o processo interno envolvido na reconstrução do agregado com o disco sobressalente. A carga de trabalho "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 de integridade do disco 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 disputa.
6. Atualize os **detalhes do evento**.

    Após a conclusão da reconstrução do RAID, verifique se o State está obsolete, indicando que o evento foi resolvido.

7. No gráfico de utilização da carga de trabalho, selecione **Bully Workloads** para visualizar as cargas de trabalho no agregado por utilização de pico.
8. Na área **Suggested Actions**, clique no botão **Analyze Workload** da carga de trabalho principal.
9. Na página **Análise de Carga de Trabalho**, defina o Intervalo de Tempo para exibir os dados das últimas 24 horas (1 dia) para o volume selecionado.

    Na Linha do Tempo de Eventos, um ponto vermelho (🔴) indica quando ocorreu o evento de falha de disco.

10. No gráfico de utilização do nó e do agregado, oculte a linha das estatísticas do nó para que apenas a linha do agregado permaneça visível.
11. Compare os dados neste gráfico com os dados no momento do evento no gráfico **Latency**.

    No momento do evento, a utilização do agregado mostra uma grande quantidade de atividade de leitura e gravação, causada pelos processos de reconstrução de RAID, o que aumentou a latência do volume selecionado. Algumas horas após a ocorrência do evento, tanto as leituras e gravações quanto a latência diminuíram, confirmando que o agregado não está mais em contenção.

Responder a um evento de desempenho causado pela tomada de controle do HA no Active IQ Unified Manager

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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Devem existir eventos de desempenho 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 afetado cuja latência foi impactada pelo componente do cluster em disputa. 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 disputa", o ícone Data Processing fica destacado em vermelho, e o nome do nó que estava processando dados no momento do evento é exibido entre parênteses.

3. Na seção **Descrição**, clique no nome do volume.

    A página Volume Performance Explorer é exibida. Na parte superior da página, na linha do tempo de Eventos, um ícone de evento de alteração ( ) indica o momento em que o Unified Manager detectou o início do takeover de HA.

4. Posicione o cursor sobre o ícone do evento de alteração do takeover de HA, e os detalhes sobre o takeover de HA serão exibidos no texto ao passar o mouse.

    No gráfico Latency, um evento indica que o volume selecionado ultrapassou o limite de desempenho devido à alta latência por volta do mesmo momento em que ocorreu o takeover de HA.

5. Clique em **Zoom View** para exibir o gráfico de latência em uma nova página.
6. No menu Exibir, selecione **Componentes do Cluster** para visualizar a latência total por componente do cluster.
7. Posicione o cursor do mouse sobre o ícone do evento de alteração para o início do takeover de HA e compare a latência do processamento de dados com a latência total.

No momento do takeover de HA, houve um pico no processamento de dados devido ao aumento da demanda da carga de trabalho no nó de processamento de dados. O aumento da utilização de CPU elevou a latência e acionou o evento.

8. Após corrigir o nó com falha, use o ONTAP System Manager para executar um HA giveback, que move as cargas de trabalho do nó parceiro para o nó corrigido.
9. Depois que o giveback de HA for concluído, após a próxima descoberta de configuração no Unified Manager (aproximadamente 15 minutos), localize o evento e a carga de trabalho acionados pelo takeover de HA na página de inventário **Event Management**.

   O evento acionado pelo takeover de 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 reduziu a latência total. O nó que o volume selecionado está usando agora para processamento de dados resolveu o evento.

Resolver eventos de desempenho

Resolva eventos de desempenho no Active IQ Unified Manager

Você pode usar as ações sugeridas para tentar resolver problemas de desempenho por conta própria. As três primeiras sugestões são sempre exibidas, e as ações da 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, de comandos da CLI do ONTAP ou de uma combinação dessas ferramentas.

Confirme se a latência está dentro da faixa esperada no Active IQ Unified Manager

Quando um componente do cluster está em contenção, as cargas de trabalho de volume que o utilizam podem apresentar tempo de resposta (latência) reduzido. Você pode revisar a latência de cada carga de trabalho afetada 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 desse volume.

Se o evento de desempenho estiver em estado obsoleto, a latência de cada vítima envolvida no evento pode ter retornado ao intervalo esperado.

Avalie como as alterações de configuração afetam o desempenho da carga de trabalho no Active IQ Unified Manager

Alterações na configuração do cluster, como um disco com falha, failover de HA ou um volume movido, podem afetar negativamente o desempenho do volume e causar aumento da latência.

No Unified Manager, você pode revisar a página Workload Analysis para ver quando ocorreu uma alteração recente na configuração e compará-la com as operações e a latência (tempo de resposta) para ver se houve alguma mudança na atividade da carga de trabalho do volume selecionado.

As páginas de desempenho do Unified Manager só conseguem detectar um número limitado de eventos de

alteração. As páginas de integridade fornecem alertas para outros eventos causados por alterações de configuração. Você pode pesquisar o volume no Unified Manager para ver o histórico de eventos.

Melhore o desempenho da carga de trabalho ajustando as configurações do lado do cliente no Active IQ Unified Manager

Você pode verificar as cargas de trabalho do seu 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 grande número de solicitações de E/S para um determinado volume 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 política de QoS ao qual o volume pertence.

Você pode investigar os clientes e seus aplicativos para determinar se os clientes estão enviando mais operações de E/S do que o normal, o que pode estar causando contenção em um componente do cluster. Na página Event details, a seção System Diagnosis exibe as principais cargas de trabalho de volume que usam o componente em contenção. Se você souber qual cliente está acessando um determinado volume, poderá acessar o cliente para determinar se o hardware do cliente ou um aplicativo não está operando conforme o esperado ou está executando 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 de outras cargas de trabalho.

Entenda como problemas de cliente ou de rede afetam o desempenho no Active IQ Unified Manager

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 de detalhes do evento, a seção Diagnóstico do sistema exibe as principais cargas de trabalho de volume que usam 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 realizando 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 possam ter feito com que as solicitações de E/S entre o cluster e os clientes conectados apresentem desempenho mais lento do que o esperado. Talvez seja necessário entrar em contato com seu administrador de rede para obter assistência.

Analise os volumes de alta atividade em um grupo de políticas de QoS no Active IQ Unified Manager

Você pode revisar as cargas de trabalho no grupo de políticas de Qualidade de Serviço (QoS) com a maior variação de atividade para determinar se mais de uma carga de trabalho causou o evento. Você também pode verificar se outras cargas de trabalho ainda estão excedendo o limite de taxa de transferência ou se já retornaram ao intervalo de atividade esperado.

Na página Detalhes do evento, na seção Diagnóstico do sistema, você pode classificar as cargas de trabalho por desvio máximo de atividade para exibir as cargas de trabalho com a maior variação de atividade no topo da tabela. Essas cargas de trabalho podem ser os “bullies” cuja atividade excedeu o limite definido e podem ter causado o evento.

Você pode acessar a página de Análise de Carga de Trabalho de cada carga de trabalho de volume para revisar sua atividade de IOPS. Se a carga de trabalho apresentar períodos de atividade operacional muito alta, isso pode ter contribuído para o evento. Você pode alterar as configurações do grupo de políticas da carga de trabalho ou movê-la para um grupo de políticas diferente.

Você pode usar o ONTAP System Manager ou os comandos da CLI do ONTAP para gerenciar grupos de políticas, conforme descrito a seguir:

- Crie um grupo de políticas.
- Adicionar ou remover cargas de trabalho em um grupo de políticas.
- Mova uma carga de trabalho entre grupos de políticas.
- Altere o limite de taxa de transferência de um grupo de políticas.

Mova os LIFs para melhorar o desempenho no Active IQ Unified Manager

Mover interfaces lógicas (LIFs) para uma porta menos utilizada 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. Ele 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 as LIFs, o que envolve movê-las 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 as LIFs ocupadas para uma porta diferente ou pode mover uma LIF manualmente.

Benefícios	Considerações
• Melhorar o balanceamento de carga. • Reduza o acesso indireto.	Ao mover uma LIF conectada a compartilhamentos CIFS, os clientes que acessam os compartilhamentos CIFS são desconectados. Quaisquer solicitações de leitura ou gravação nos compartilhamentos CIFS são interrompidas.

Você usa os comandos do ONTAP para configurar o balanceamento de carga. Para obter mais informações, consulte a documentação de rede do ONTAP.

Você usa o ONTAP System Manager e os comandos da ONTAP CLI para mover LIFs manualmente.

Execute operações de eficiência de storage em horários menos movimentados

Agende operações de eficiência de storage para horários de menor movimento no Active IQ Unified Manager

Você pode modificar a política ou o agendamento que gerencia as operações de eficiência de storage para que sejam executadas quando as cargas de trabalho do volume afetado estiverem menos ocupadas.

As operações de eficiência de storage podem consumir muitos recursos da CPU do cluster e sobrecarregar os volumes nos quais as operações estão sendo executadas. Se os volumes afetados apresentarem alta atividade ao mesmo tempo em que as operações de eficiência de storage são executadas, sua latência pode aumentar e desencadear um evento.

Na página de detalhes do evento, a seção System Diagnosis exibe as cargas de trabalho no grupo de política de QoS por desvio máximo na atividade para identificar as cargas de trabalho agressoras. Se você vir “storage efficiency” exibido próximo ao topo da tabela, essas operações estão prejudicando as cargas de trabalho vítimas. Ao modificar a política de eficiência ou o agendamento para executar quando essas cargas de trabalho estiverem menos ocupadas, você pode evitar que as operações de eficiência de storage causem contenção em um cluster.

Você pode usar o ONTAP System Manager para gerenciar políticas de eficiência. Você pode usar os comandos do ONTAP para gerenciar políticas e agendamentos de eficiência.

Entenda a eficiência de storage no Active IQ Unified Manager

A eficiência de storage permite que você armazene a quantidade máxima de dados com o menor custo e acomoda o rápido crescimento de dados, consumindo menos espaço. A estratégia da NetApp para eficiência de storage baseia-se na base incorporada de virtualização de storage e storage unificado fornecida pelo seu principal sistema operacional ONTAP e pelo sistema de arquivos WAFL.

A eficiência de storage inclui o uso de tecnologias como thin provisioning, cópia Snapshot, deduplicação, compressão de dados, FlexClone, thin replication com SnapVault e volume SnapMirror, RAID-DP, Flash Cache, agregado Flash Pool e agregados habilitados para FabricPool, que ajudam a aumentar a utilização do storage e diminuir os custos de armazenamento.

A arquitetura de storage unificado permite consolidar de forma eficiente uma rede de área de armazenamento (SAN), um armazenamento conectado à rede (NAS) e storage secundário em uma plataforma única.

Unidades de disco de alta densidade, como unidades SATA (Serial Advanced Technology Attachment) configuradas em agregados do Flash Pool ou com o Flash Cache e a tecnologia RAID-DP, aumentam a eficiência sem afetar o desempenho e a resiliência.

Um agregado habilitado para FabricPool inclui um agregado totalmente SSD ou um agregado HDD (a partir do 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 storage (a camada local ou a camada de nuvem) os dados devem ser armazenados com base em serem acessados com frequência.

Tecnologias como thin provisioning, cópia Snapshot, deduplicação, compressão de dados, thin replication com

SnapVault e volume SnapMirror, e FlexClone oferecem maior economia. Você pode usar essas tecnologias individualmente ou em conjunto para obter a máxima eficiência de storage.

Entenda como a adição de discos afeta a realocação de dados no Active IQ Unified Manager

Você pode adicionar discos a um agregado para aumentar a capacidade de storage e o desempenho desse agregado. Após adicionar os discos, você verá uma melhoria no desempenho de leitura somente depois de realocar os dados entre os discos que você adicionou.

Você pode usar estas instruções quando o Unified Manager tiver recebido eventos de agregado acionados por limites dinâmicos ou por limites de desempenho definidos pelo sistema:

- Quando você recebe um evento de limite dinâmico, na página de detalhes do evento, o ícone do componente do cluster que representa o agregado em disputa fica 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 de 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 adicionar ao agregado já devem existir no cluster. Se o cluster não tiver discos adicionais disponíveis, talvez seja necessário entrar em contato com seu administrador ou adquirir mais discos. Você pode usar o ONTAP System Manager ou os comandos do 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.

Melhore o desempenho da carga de trabalho ativando o Flash Cache em um nó no Active IQ Unified Manager

Você pode melhorar o desempenho da carga de trabalho ativando o Flash Cache™ para armazenamento em cache inteligente de dados em cada nó do cluster.

Um módulo Flash Cache, ou um módulo de memória baseado em PCIe Performance Acceleration Module, otimiza o desempenho de cargas de trabalho com uso intensivo de leitura aleatória ao funcionar 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 de 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 do 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 utilizá-lo, consulte o seguinte relatório

técnico:

"Relatório Técnico 3832: o Guia de Práticas Recomendadas do Flash Cache"

Melhore o desempenho da carga de trabalho ativando o Flash Pool em um agregado de storage no Active IQ Unified Manager

Você pode melhorar o desempenho da carga de trabalho ativando o recurso do Flash Pool em um agregado. O Flash Pool é um agregado que incorpora HDDs e SSDs. Os HDDs são usados para storage primário, e os SSDs fornecem um cache de leitura e gravação de alto desempenho para aumentar o desempenho do agregado.

No Unified Manager, a página de detalhes do evento exibe o nome do agregado em contenção. Você pode usar o ONTAP System Manager ou os comandos do 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-lo. 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 *Clustered Data ONTAP Physical Storage Management Guide*.

Verifique a integridade da configuração do MetroCluster no Active IQ Unified Manager

Você pode usar o Unified Manager para analisar a integridade dos clusters em uma configuração MetroCluster por IP ou FC. O status de integridade e os eventos ajudam você a determinar se há problemas de hardware ou software que possam estar afetando o desempenho das suas cargas de trabalho.

Se você configurar o Unified Manager para enviar alertas por e-mail, poderá verificar seu e-mail para identificar 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 **Event Management** para ver uma lista dos 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"

Verifique as configurações do MetroCluster no Active IQ Unified Manager

É possível evitar problemas de desempenho em cargas de trabalho espelhadas em uma configuração do MetroCluster por FC e IP, garantindo que a configuração do MetroCluster esteja correta. Também é possível melhorar o desempenho da carga de trabalho alterando a configuração ou atualizando componentes de software ou hardware.

Consulte "Documentação do MetroCluster" as instruções para configurar os clusters na configuração do MetroCluster, incluindo os switches Fibre Channel (FC), os cabos e os 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 sua configuração de MetroCluster over IP, consulte "Instale uma configuração IP do MetroCluster".

Você pode comparar sua configuração do MetroCluster com os requisitos em "Documentação do MetroCluster" para determinar se alterar ou atualizar componentes em sua configuração do MetroCluster pode melhorar o desempenho da carga de trabalho. Essa comparação pode ajudar você a responder às seguintes perguntas:

- Os controladores são adequados para suas cargas de trabalho?
- Você precisa atualizar seus pacotes ISL para uma largura de banda maior para suportar um throughput mais alto?
- É possível ajustar os créditos de buffer a buffer (BBC) nos seus switches para aumentar a largura de banda?
- Se suas cargas de trabalho tiverem alta taxa de transferência de gravação para armazenamento em unidade de estado sólido (SSD), você precisa atualizar suas pontes FC-para-SAS para suportar essa taxa de transferência?

Informações relacionadas

- Para obter informações sobre como substituir ou atualizar os componentes do MetroCluster, consulte o "Documentação do MetroCluster".
- Para obter informações sobre como atualizar controladores consulte "Atualização de controladores em uma configuração FC do MetroCluster usando switchover e switchback" e "Atualização de controladores em uma configuração IP do MetroCluster usando switchover e switchback"

Mova as cargas de trabalho para um agregado diferente no Active IQ Unified Manager

Você pode usar o Unified Manager para ajudar a identificar um agregado menos ocupado do que o agregado em que suas cargas de trabalho residem atualmente e, em seguida, mover volumes ou LUNs selecionados para esse agregado. Mover cargas de trabalho de alto desempenho para um agregado menos ocupado ou para um agregado com storage flash habilitado permite que a carga de trabalho tenha melhor desempenho.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Você deve ter registrado o nome do agregado que está apresentando problemas de desempenho no momento.
- Você deve ter registrado a data e a hora em que o agregado recebeu o evento.
- O Unified Manager deve ter coletado e analisado dados de desempenho referentes a um mês ou mais.

Estas etapas ajudam você a identificar os seguintes recursos para que possa mover cargas de trabalho de alto desempenho para um agregado com menor utilização:

- Os agregados no mesmo cluster que são menos utilizados
- Os volumes de melhor desempenho no agregado atual

Passos

1. Identifique o agregado no cluster que é o menos utilizado:
   a. Na página de detalhes do **Evento**, clique no nome do cluster no qual o agregado está localizado.

      Os detalhes do cluster são exibidos na página de destino Desempenho/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 possuem a maior **Capacidade Livre**. Isso fornece uma lista de agregados potenciais 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 do agregado são exibidos na página Performance/Aggregate Explorer.

   b. No seletor **Intervalo de tempo**, selecione **Últimos 30 dias** e clique em **Aplicar intervalo**.

      Isso permite visualizar um período de histórico de desempenho mais longo do que as 72 horas padrão. Você pode querer mover um volume que esteja usando muitos recursos de forma consistente, e não apenas nas últimas 72 horas.

   c. No controle **Exibir e Comparar**, selecione **Volumes deste Agregado**.

      É exibida uma lista dos volumes FlexVol e dos volumes constituintes FlexGroup neste agregado.

   d. Ordene os volumes pelo maior valor em MB/s e, em seguida, pelo maior valor em IOPS, para visualizar os volumes com melhor desempenho.
   e. Anote os nomes dos volumes que você deseja mover para um agregado diferente.
3. Transfira 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, comandos do ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, verifique se você está recebendo o mesmo tipo de eventos deste nó ou agregado.

Mova as cargas de trabalho para um nó diferente no Active IQ Unified Manager

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 atualmente e, em seguida, 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 sejam executadas com mais eficiência.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- 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 possa mover cargas de trabalho de alto desempenho para um nó menos utilizado:

- Os nós no mesmo cluster que possuem a maior capacidade de desempenho livre
- Os agregados no novo nó que possuem a maior capacidade de desempenho livre
- Os volumes de melhor 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 está localizado.

      Os detalhes do cluster são exibidos na página de destino Desempenho/Cluster.

   b. Na guia **Summary**, clique em **Nodes** no painel **Managed Objects**.

      A lista de nós neste cluster é exibida.

   c. Clique na coluna **Capacidade de desempenho utilizada** para classificar os nós por menor percentual de utilização.

      Isso fornece uma lista de nós potenciais para os quais você pode querer mover cargas de trabalho.

   d. Anote o nome do nó para o qual você deseja mover as cargas de trabalho.
2. Identifique um agregado no novo nó que seja o menos utilizado:
   a. No painel de navegação à esquerda, clique em **Armazenamento** > **Agregados** e selecione **Desempenho** > **Todos os Agregados** no menu **Exibir**.

      A visualização Performance: All Aggregates 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 visualização Performance: All Aggregates é exibida novamente com a lista de agregados disponíveis neste nó.

   c. Clique na coluna **Capacidade de desempenho utilizada** para classificar os agregados por menor utilização.

      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 à página **Detalhes do evento** do evento.
   b. No campo **Volumes afetados**, clique no link do número de volumes.

      A visualização Desempenho: todos os volumes exibe 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 possíveis volumes que você pode querer mover.

d. Anote os nomes dos volumes que você deseja mover e os nomes dos agregados atuais nos quais eles se encontram.

4. Mova os volumes para os agregados que você identificou como tendo a maior capacidade de desempenho livre no novo nó.

   Você pode executar a operação de movimentação usando o ONTAP System Manager, o OnCommand Workflow Automation, comandos do ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, você poderá verificar se está recebendo o mesmo tipo de eventos desse nó ou agregado.

Mova as cargas de trabalho para um agregado em um nó diferente no Active IQ Unified Manager

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 atualmente e, em seguida, 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- 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 referentes a um mês ou mais.

Estas etapas ajudam você a identificar os seguintes recursos para que possa mover cargas de trabalho de alto desempenho para um nó menos utilizado:

- Os nós do mesmo cluster que estão menos utilizados
- Os agregados no novo nó que são menos utilizados
- Os volumes de melhor desempenho no nó atual

Passos

1. Identifique o nó menos utilizado no cluster:
   a. Na página de detalhes do **Evento**, clique no nome do cluster em que o nó está localizado.

      Os detalhes do cluster são exibidos na página de destino Desempenho/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 por ordem de menor utilização.

      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 à esquerda, clique em **Armazenamento** > **Agregados** e selecione **Desempenho** > **Todos os Agregados** no menu **Exibir**.

      A visualização Performance: All Aggregates 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 visualização Performance: All Aggregates 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 possuem a maior **Capacidade Livre**. Isso fornece uma lista de agregados potenciais 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. Volte para a página de detalhes do **Event** do evento.
   b. No campo **Volumes afetados**, clique no link do número de volumes.

      A visualização Desempenho: todos os volumes exibe 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 possíveis volumes que você pode querer mover.

   d. Anote os nomes dos volumes que você deseja mover e os nomes dos agregados atuais nos quais eles se encontram.
4. Transfira os volumes para os agregados que você identificou com baixa utilização no novo nó.

   Você pode executar a operação de movimentação usando o ONTAP System Manager, o OnCommand Workflow Automation, comandos do ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, verifique se você está recebendo o mesmo tipo de eventos deste nó ou agregado.

Mova as cargas de trabalho para um nó em um par de HA diferente no Active IQ Unified Manager

Você pode usar o Unified Manager para ajudar a identificar um agregado em um nó de 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 são executadas atualmente. Em seguida, você pode mover os volumes selecionados para agregados no novo par de HA.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Seu cluster deve consistir em no mínimo dois pares de HA

  Não é possível usar este processo de correção se você tiver apenas um par de HA no seu cluster.

- Você deve ter anotado os nomes dos dois nós do par de 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 possa mover cargas de trabalho de alto desempenho para um nó que tenha mais capacidade de desempenho livre em um par de HA:

- 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 possuem a maior capacidade de desempenho livre
- Os volumes de melhor desempenho nos nós atuais

Passos

1. Identifique os nós que fazem parte de um par de HA diferente no mesmo cluster:
   a. Na página **Detalhes do Evento**, clique no nome do cluster em que os nós estão localizados.

      Os detalhes do cluster são exibidos na página de destino Desempenho/Cluster.

   b. Na página **Resumo**, clique em **Nós** no painel **Objetos gerenciados**.

      A lista de nós neste cluster é exibida na visualização 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 de HA que tenha a maior capacidade de desempenho livre:
   a. Na visualização **Desempenho: todos os nós**, clique na coluna **Capacidade de desempenho utilizada** para classificar os nós por menor percentual de utilização.

      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 visualização **Desempenho: todos os nós**, clique no nó.

      Os detalhes do nó são exibidos na página Performance/Node Explorer.

   b. No menu **Exibir e Comparar**, selecione **Agregados neste Nó**.

      Os agregados neste nó são exibidos na grade.

   c. Clique na coluna **Capacidade de desempenho utilizada** para classificar os agregados por menor utilização.

      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 nos nós que receberam o evento:

a. Volte para a página de detalhes do **Event** do evento.
b. No campo **Volumes Afetados**, clique no link correspondente ao número de volumes do primeiro nó.

   A visualização Desempenho: todos os volumes exibe 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 em potencial que você pode querer mover.

d. Anote os nomes dos volumes que você deseja mover e os nomes dos agregados atuais nos quais eles se encontram.
e. Execute os passos 4c e 4d para o segundo nó que fez parte deste evento para identificar possíveis volumes que você também deseja mover desse nó.

5. Mova os volumes para os agregados que você identificou como tendo a maior capacidade de desempenho livre no novo nó.

   Você pode executar a operação de movimentação usando o ONTAP System Manager, o OnCommand Workflow Automation, comandos do ONTAP ou uma combinação dessas ferramentas.

Após alguns dias, você poderá verificar se está recebendo o mesmo tipo de eventos desse nó ou agregado.

Mova as cargas de trabalho para outro nó em um par de HA no Active IQ Unified Manager

Você pode usar o Unified Manager para ajudar a identificar um agregado em um nó de um par de HA diferente que esteja menos ocupado do que o par de HA onde suas cargas de trabalho estão sendo executadas atualmente. Em seguida, você pode mover volumes selecionados para agregados no novo par de 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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Seu cluster deve consistir em no mínimo dois pares de HA; você não pode usar este processo de correção se tiver apenas um par de HA em seu cluster.
- Você deve ter anotado os nomes dos dois nós do par de HA que estão apresentando o problema 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 referentes a um mês ou mais.

Estas etapas ajudam você a identificar os seguintes recursos para que possa mover cargas de trabalho de alto desempenho para um nó menos utilizado em um par de HA diferente:

- Os nós em um par de HA diferente no mesmo cluster que são menos utilizados
- Os agregados nos novos nós que são menos utilizados
- Os volumes de melhor desempenho nos nós atuais

Passos

1. Identifique os nós que fazem parte de um par de HA diferente no mesmo cluster:
   a. No painel de navegação à esquerda, 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 **Node Count** 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 de HA que seja o menos utilizado:
   a. Clique na coluna **Utilização** para classificar os nós por ordem de menor utilização.

      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 à esquerda, clique em **Armazenamento** > **Agregados** e selecione **Desempenho** > **Todos os Agregados** no menu **Exibir**.

      A visualização Performance: All Aggregates 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 visualização Performance: All Aggregates 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 possuem a maior **Capacidade Livre**. Isso fornece uma lista de agregados potenciais 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 nos nós que receberam o evento:
   a. Volte para a página de detalhes do **Event** do evento.
   b. No campo **Volumes Afetados**, clique no link correspondente ao número de volumes do primeiro nó.

      A visualização Desempenho: todos os volumes exibe 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 em potencial que você pode querer mover.

   d. Anote os nomes dos volumes que você deseja mover e os nomes dos agregados atuais nos quais eles se encontram.
   e. Execute os passos 4c e 4d para o segundo nó que fez parte deste evento para identificar possíveis volumes que você também deseja mover desse nó.

5. Transfira os volumes para os agregados que você identificou com baixa utilização no novo nó.

   Você pode executar a operação de movimentação usando o ONTAP System Manager, o OnCommand Workflow Automation, comandos do 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 as cargas de trabalho dos nós no Active IQ Unified Manager

Você pode definir um limite em um grupo de políticas de QoS para controlar o limite de I/O por segundo (IOPS) ou o limite de taxa de transferência em 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 pode 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 e podem ter contribuído para o evento.

Ao atribuir os volumes que estão sobrecarregando 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 nesse nó.

Você pode usar o ONTAP System Manager ou os comandos do 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
- Transferir carga de trabalho entre grupos de políticas
- Alterando o limite de taxa de transferência de um grupo de políticas

Remova volumes e LUNs inativos no Active IQ Unified Manager

Quando o espaço livre do agregado for identificado como um problema, você pode 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 de disco, existem algumas maneiras de determinar quais volumes e LUNs não estão mais sendo usados.

Para identificar volumes não utilizados:

- Na página de detalhes do evento, o campo **Affected Objects Count** 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 estiveram ativos.

Para identificar LUNs não utilizadas:

1. Na página de detalhes do evento, anote o nome do agregado no qual o evento ocorreu.
2. No painel de navegação esquerdo, clique em **Armazenamento** > **LUNs** e selecione **Desempenho** > **Todos os LUNs** no menu Exibir.
3. Clique em **Filtragem**, selecione **Agregado** no menu suspenso à esquerda, digite o nome do agregado no campo de texto e clique em **Aplicar filtro**.
4. Ordene a lista resultante de LUNs afetados por **IOPS** para visualizar os LUNs que não estão ativos.

Após identificar os volumes e LUNs não utilizados, você pode usar o ONTAP System Manager ou os comandos do ONTAP para excluir esses objetos.

Entenda como a adição de discos afeta o layout do agregado no Active IQ Unified Manager

Você pode adicionar discos a um agregado para aumentar a capacidade de storage e o desempenho desse agregado. Após adicionar os discos, você só verá uma melhoria no desempenho depois de reconstruir o agregado.

Ao receber um evento de limite definido pelo sistema na página Detalhes do evento, o texto de descrição do evento lista o nome do agregado que está apresentando o problema. Você pode adicionar discos e reconstruir os dados nesse agregado.

Os discos que você adicionar ao agregado já devem existir no cluster. Se o cluster não tiver discos adicionais disponíveis, talvez seja necessário entrar em contato com seu administrador ou adquirir mais discos. Você pode usar o ONTAP System Manager ou os comandos do ONTAP para adicionar discos a um agregado.

"Relatório Técnico 3838: guia de Configuração do Subsistema de Armazenamento"

Configure uma conexão entre um servidor Unified Manager e um provedor de dados externo

Configure uma conexão entre o Active IQ Unified Manager e um provedor de dados externo

Uma conexão entre o servidor do Unified Manager e um provedor externo de dados permite enviar dados de desempenho do cluster para um servidor externo, para que os administradores de storage possam gerar gráficos das 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 “External Data Provider” no console de manutenção.

Envie os dados de desempenho do Active IQ Unified Manager para um servidor externo

O Unified Manager coleta diversos 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 visualizar no gráfico, você pode optar por enviar um dos seguintes grupos de estatísticas:

Grupo de estatísticas	Dados incluídos	Detalhes
Performance Monitor	Estatísticas de desempenho de alto nível para os seguintes objetos: • LUNs • Volumes	Este grupo fornece o total de IOPS ou latência 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 os recursos físicos do agregado em todos os clusters monitorados. Também fornece as estatísticas coletadas no grupo Performance Monitor.
Detalhamento	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. 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 de um objeto de cluster for alterado no sistema de storage, tanto o objeto antigo quanto o novo conterão dados de desempenho no servidor externo (chamado de “metric_path”). Os dois objetos não são tratados como o mesmo objeto. Por exemplo, se você alterar o nome de um volume de “volume1_acct” para “acct_vol1”, você verá dados de desempenho antigos para o volume antigo e dados de desempenho novos para o volume novo.

Consulte o artigo da Knowledge Base 30096 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"

Configure o Graphite para receber dados de desempenho do Active IQ Unified Manager

O Graphite é uma ferramenta de software livre para coletar e gerar gráficos de dados de desempenho de sistemas de computador. Seu servidor e software Graphite devem estar

configurados corretamente para receber dados estatísticos do Unified Manager.

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.

Após instalar o Graphite de acordo com as instruções de instalação, você precisa fazer as seguintes alterações para oferecer 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 ser necessário criar inicialmente milhares de novos arquivos. 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 deixa de ser relevante.

- Se você estiver executando o Graphite em um servidor implantado usando um endereço IPv6, o valor de LINE_RECEIVER_INTERFACE no `/opt/graphite/conf/carbon.conf` arquivo deve ser alterado de "0.0.0.0" para "::" (**`LINE_RECEIVER_INTERFACE = ::`**
- No `/opt/graphite/conf/storage-schemas.conf` arquivo, o `retentions` parâmetro deve ser usado para definir a frequência para 5 minutos e o período de retenção para o número de dias relevante para o seu ambiente.

  O período de retenção pode ser tão longo quanto o seu ambiente permitir, mas o valor da 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 como 5 minutos e o período de retenção como 100 dias: `**[OPM]**

  ```
  pattern = ^netapp-performance\..

  retentions = 5m:100d
  ```

  Se a tag de fornecedor padrão for alterada de "netapp-performance" para algo diferente, essa alteração também deverá ser refletida no parâmetro `pattern`.

Se o servidor Graphite estiver indisponível quando o servidor do Unified Manager tentar enviar dados de desempenho, os dados não serão enviados e haverá uma lacuna nos dados coletados.

Configure uma conexão entre o Active IQ Unified Manager e 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 a serem enviados e o intervalo de envio.

Antes de começar

- Você precisa ter um ID de usuário autorizado para fazer login no console de manutenção do servidor Unified Manager.
- Você deve ter as seguintes informações sobre o fornecedor 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 terceiro para que ele possa receber dados estatísticos do servidor do Unified Manager.
- Você precisa saber qual grupo de estatísticas deseja enviar:
  - PERFORMANCE_INDICATOR: estatísticas do monitor de desempenho
  - RESOURCE_UTILIZATION: utilização de recursos e estatísticas do monitor de desempenho
  - DETALHAMENTO: todas as estatísticas
- Você precisa 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 enviada durante cada transmissão será duas (ou três) vezes maior do que quando você usa 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 ele seja igual ou maior que o intervalo de coleta do Unified Manager.

Você pode configurar uma conexão entre um servidor Unified Manager e um servidor provedor de dados externo.

Passos

1. Faça login como o usuário de manutenção no console de manutenção do servidor do Unified Manager.

   Os avisos do console de manutenção do Unified Manager são exibidos.

2. No console de manutenção, digite o número da opção de menu **Fornecedor de Dados Externos**.

   O menu Conexão com Servidor Externo é exibido.

3. Digite o número da opção de menu **Adicionar/Modificar Conexão com o 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 de conexão com servidor externo.
8. Digite o número da opção de menu **Modificar configuração do servidor**.

   Você vê as informações atuais de configuração do servidor.

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 serão enviadas e se deseja ativar a transmissão de estatísticas agora:

Para..	Digite…
ID do grupo de estatísticas	`0` - INDICADOR_DE_DESEMPENHO (padrão) `1` - UTILIZAÇÃO DE RECURSOS `2` - DRILL_DOWN
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. Utilizando a notação de ponto, você pode definir uma estrutura de pastas hierárquica. Por exemplo, ao inserir `stats.performance.netapp` as estatísticas ficarão em **stats** > **performance** > **netapp**.
Intervalo de transmissão	`5` (padrão), `10`, ou `15` minutos
Ativar/desativar	`0` - Desativar `1` - Ativar (padrão)

11. Quando solicitado, digite `y` para verificar se as informações inseridas estão corretas.
12. Pressione qualquer tecla para retornar ao menu de conexão com servidor externo.
13. Digite `x` para sair do console de manutenção.

Após configurar a conexão, os dados de desempenho selecionados são enviados para o servidor de destino no intervalo de tempo especificado. Leva alguns minutos para que as métricas comecem a aparecer na ferramenta externa. Pode ser necessário atualizar o 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

Saiba mais sobre o monitoramento de integridade do Active IQ Unified Manager

O Active IQ Unified Manager (anteriormente o 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 de servidor do Unified Manager oferece escalabilidade, suporte e recursos aprimorados de monitoramento e notificação.

As principais funcionalidades do Unified Manager incluem monitoramento, emissão de alertas, gerenciamento da disponibilidade e da capacidade dos clusters, gerenciamento de recursos de proteção e agrupamento de dados de diagnóstico e envio deles ao 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 executar para solucionar os problemas. Você pode configurar alertas para eventos para que, quando ocorrerem problemas, você receba notificações 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 a essas anotações por meio de regras.

Você também pode planejar os requisitos de armazenamento dos objetos do seu cluster usando as informações fornecidas nos gráficos de capacidade e saúde do respectivo objeto de cluster.

Capacidade física e lógica

O Unified Manager utiliza os conceitos de espaço físico e lógico usados para objetos de storage do ONTAP.

- Capacidade física: o espaço físico refere-se aos blocos físicos de armazenamento utilizados no volume. A "capacidade física utilizada" é normalmente menor que a capacidade lógica utilizada devido à redução de dados dos recursos de eficiência de storage, como deduplicação e compressão.
- Capacidade lógica: o espaço lógico refere-se ao espaço utilizável (os blocos lógicos) em um volume. O espaço lógico refere-se a como o espaço teórico pode ser usado, sem considerar os resultados da deduplicação ou da compressão. O "espaço lógico usado" é o espaço físico usado mais a economia gerada pelos recursos de eficiência de storage, como deduplicação e compressão, que foram configurados. Essa medição geralmente parece maior do que a capacidade física usada porque não reflete a compressão de dados e outras reduções no espaço físico. Assim, a capacidade lógica total pode ser maior do que o espaço provisionado.

Unidades de medida de capacidade

O Unified Manager calcula a capacidade de storage 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, elas são exibidas no Unified Manager como KiB, MiB, GiB, TiB e PiB.

As unidades usadas para a taxa de transferência continuam sendo kilobytes por segundo (Kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) ou terabytes por segundo (Tbps) e assim por diante, para todas as versões do ONTAP.

Unidade de capacidade exibida no 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
TB	TiB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 bytes

Entenda os recursos de monitoramento de integridade do Active IQ Unified Manager

O Unified Manager é construído 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 com o software ONTAP instalado:
  - Objetos físicos: nós, discos, gavetas de discos, pares SFO, portas e o Flash Cache
  - Objetos lógicos: clusters, máquinas virtuais de storage (SVMs), agregados, volumes, LUNs, namespaces, qtrees, LIFs, cópias Snapshot, caminhos de junção, compartilhamentos NFS, compartilhamentos SMB, cotas de usuário e grupo, grupos de política de QoS e grupos de iniciadores
  - Protocolos: CIFS, NFS, FC, iSCSI, NVMe e FCoE
  - Eficiência de storage: agregados SSD, agregados do Flash Pool, agregados do FabricPool, deduplicação e compressão
  - Proteção: relacionamentos do SnapMirror (síncronos e assíncronos) e relacionamentos do SnapVault
- Visualizando o status de descoberta e monitoramento do cluster
- Configurações do MetroCluster over FC e IP: exibição e monitoramento da configuração, de problemas e do status de conectividade dos componentes do cluster. Switches e bridges do MetroCluster para configurações do MetroCluster over FC
- Infraestrutura aprimorada de alertas, eventos e limites
- LDAP, LDAPS, autenticação SAML e suporte a usuários locais
- RBAC (para um conjunto predefinido de papéis)
- O AutoSupport e o pacote de suporte
- Painel de controle aprimorado para exibir a capacidade, a disponibilidade, a proteção e o desempenho do ambiente

- Interoperabilidade de movimentação de volume, histórico de movimentação de volume e histórico de alteração de caminho de junção
- Área de Escopo de Impacto que exibe graficamente os recursos afetados por eventos como "Alguns discos com falha", MetroCluster Aggregate Mirroring Degraded e MetroCluster Spare Disks Left Behind
- Área de possíveis efeitos que exibe o efeito dos eventos do MetroCluster
- A área Ações corretivas sugeridas exibe as ações que podem ser executadas para solucionar eventos como Alguns discos com falha, MetroCluster Espelhamento de agregado degradado e MetroCluster Discos sobressalentes deixados para trás
- A seção Recursos que podem ser afetados exibe os recursos que podem ser impactados por eventos como o evento Volume Offline, o evento Volume Restricted e o evento Thin-Provisioned Volume Space At Risk
- Suporte para SVMs com volumes FlexVol ou FlexGroup
- Suporte para monitoramento de volumes raiz de nós
- Monitoramento aprimorado de cópias Snapshot, incluindo a computação do espaço recuperável e a exclusão de cópias Snapshot
- Anotações para objetos de storage
- Criação e gerenciamento de relatórios com informações sobre objetos de storage, como capacidade física e lógica, utilização, economia de espaço, desempenho e eventos relacionados
- Integração com o OnCommand Workflow Automation para executar fluxos de trabalho

  "Download WFA"

Use as interfaces do Active IQ Unified Manager para gerenciar a integridade do sistema de storage

Estas seções contêm informações sobre as duas interfaces de usuário que o Active IQ Unified Manager oferece para solucionar problemas de capacidade, disponibilidade e proteção no storage de dados. As duas interfaces de usuário são a interface da Web do Unified Manager e o console de manutenção.

Se você deseja usar os recursos de proteção do Unified Manager, também precisa 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 do cluster relacionados à capacidade de storage, disponibilidade e proteção de dados.

Estas seções descrevem alguns fluxos de trabalho comuns que um administrador pode seguir para solucionar problemas de capacidade de storage, disponibilidade de dados ou proteção exibidos na interface 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 de usuários e problemas de rede relacionados ao próprio servidor do Unified Manager. Se a interface web do Unified Manager estiver indisponível, 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 utilizá-las para resolver problemas relacionados ao funcionamento do servidor Unified Manager.

Gerenciar e monitorar clusters e a integridade dos objetos do cluster

Entenda o monitoramento de clusters

Entenda o monitoramento de clusters no Active IQ Unified Manager

Você pode adicionar clusters ao banco de dados do Unified Manager para monitorar os clusters quanto à disponibilidade, à capacidade e a outros detalhes, como uso da CPU, estatísticas da interface, espaço de disco livre, uso de qtree e ambiente do chassi.

Os eventos são gerados se o status for anormal ou quando um limite predefinido for ultrapassado. Se estiver configurado para isso, o Unified Manager envia uma notificação a um destinatário especificado quando um evento aciona um alerta.

Compreenda os volumes raiz dos nós no Active IQ Unified Manager

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 saia do ar.

Quando a capacidade usada do volume raiz do nó excede 80 por cento da capacidade total do volume raiz do nó, o evento "Node Root Volume Space Nearly Full" é gerado. Você pode configurar um alerta para o evento e receber uma notificação. Você pode tomar as medidas apropriadas para evitar que o nó fique inativo usando o ONTAP System Manager ou a ONTAP CLI.

A funcionalidade de monitoramento de volumes raiz de nós não está disponível se os clusters executarem a versão ONTAP 9.14.1 ou posterior.

Compreenda os eventos e limites para agregados de raiz de nó no Active IQ Unified Manager

Você pode monitorar o agregado de raiz do nó usando o Unified Manager. A melhor prática é fazer o provisionamento thick do volume raiz no agregado de raiz para evitar que o nó pare.

Por padrão, eventos de capacidade e desempenho não são gerados para agregados de raiz. Além disso, os valores de limite usados pelo Unified Manager não se aplicam aos agregados de raiz dos nós. Somente um representante do suporte técnico pode modificar as configurações para que esses eventos sejam gerados. Quando as configurações são modificadas por um representante do suporte técnico, os valores de limite de capacidade são aplicados ao agregado de raiz do nó.

Você pode tomar as medidas apropriadas para evitar que o nó pare usando o ONTAP System Manager ou a ONTAP CLI.

A funcionalidade de monitoramento de agregados de raiz de nós não está disponível se os clusters executarem a versão 9.14.1 do ONTAP ou posterior.

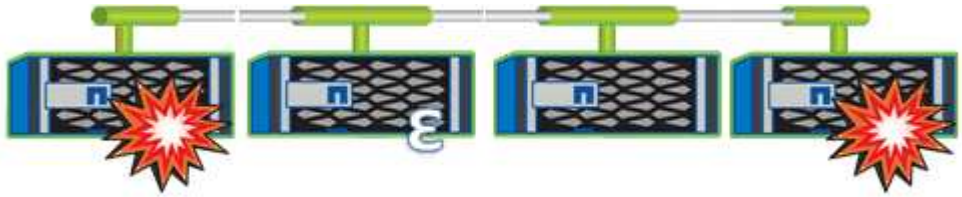
Entenda o quorum e o epsilon em clusters ONTAP no Active IQ Unified Manager

Quorum e epsilon são medidas importantes da saúde e do funcionamento do cluster, que juntas indicam como os clusters lidam com possíveis desafios de comunicação e conectividade.

O *quorum* é uma pré-condição para o pleno funcionamento de um cluster. Quando um cluster está em quorum, a maioria simples dos nós está íntegra e consegue se comunicar entre si. Quando o quorum é perdido, o cluster perde a capacidade de realizar as operações normais do cluster. Apenas um conjunto de nós pode ter quorum por vez, porque todos os nós compartilham coletivamente uma única visão dos dados. Portanto, se for permitido que dois nós sem comunicação modifiquem os dados de maneiras divergentes, não será mais possível reconciliar os dados em uma única visão dos dados.

Cada nó no cluster participa de um protocolo de votação que elege um nó mestre; cada nó restante é um nó secundário. O nó mestre é responsável por sincronizar as 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 em quórum, um novo mestre é eleito pelos nós que permanecem online.

Como existe a possibilidade de empate em um cluster com um número par de nós, um nó tem um peso de voto fracionário extra chamado epsilon. Se a conectividade entre duas partes iguais de um cluster grande falhar, o grupo de nós que contém epsilon mantém o quórum, desde que todos os nós estejam íntegros. Por exemplo, a ilustração a seguir mostra um cluster de quatro nós no qual dois dos nós falharam. No entanto, como um dos nós sobreviventes detém epsilon, o cluster permanece em quórum, embora não haja uma maioria simples de nós íntegros.



O Epsilon é atribuído automaticamente ao primeiro nó quando o cluster é criado. Se o nó que mantém o Epsilon ficar não íntegro, assumir o controle do parceiro de alta disponibilidade ou passar a ser controlado por ele, o Epsilon será automaticamente reatribuído a um nó íntegro em um par de HA diferente.

Colocar um nó offline pode afetar a capacidade do cluster de permanecer em quórum. Portanto, o ONTAP emite uma mensagem de aviso se você tentar uma operação que retire o cluster do quórum ou o deixe a apenas uma interrupção da perda de quórum. Você pode desativar as mensagens de aviso de quórum 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 do que um cluster menor. O requisito de quórum, que consiste em uma maioria simples de metade dos nós mais um épsilon, 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 exclusivos para manter o quórum. Clusters de dois nós usam HA de cluster, em que nenhum dos nós detém epsilon; em vez disso, ambos os nós são consultados continuamente para garantir que, se um nó falhar, o outro tenha acesso completo de leitura e gravação aos dados, bem como acesso às interfaces lógicas e às funções de gerenciamento.

Visualize a lista de clusters e detalhes no Active IQ Unified Manager

Você pode usar a visualização Health: All Clusters para ver seu inventário de clusters. A

visualização Capacity: All Clusters permite que você veja informações resumidas sobre a capacidade de storage e a utilização em todos os clusters.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Você também pode ver detalhes de clusters individuais, como a integridade, a capacidade, a configuração, as LIFs, os nós e os discos desse cluster, usando a página de detalhes Cluster / Health.

Os detalhes na visualização Saúde: todos os clusters, na visualização Capacidade: todos os clusters e na página de detalhes Cluster / Saúde ajudam você a planejar seu storage. Por exemplo, antes de provisionar um novo agregado, você pode selecionar um cluster específico na visualização Saúde: 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 visualização **Health: All Clusters** para ver informações de integridade ou a visualização **Capacity: All Clusters** para ver detalhes sobre a capacidade de storage e a utilização em todos os clusters.
3. Clique no nome de um cluster para visualizar os detalhes completos do cluster na página de detalhes **Cluster / Health**.

Informações relacionadas

- "Página de detalhes de cluster / saúde"
- "Desempenho: visualização de todos os clusters"
- "Monitoramento de configurações do MetroCluster"
- "Visualizando o status de segurança para clusters e VMs de armazenamento"
- "Quais critérios de segurança estão sendo avaliados"

Verifique a integridade dos clusters em uma configuração MetroCluster no Active IQ Unified Manager

Você pode usar o Active IQ Unified Manager (Unified Manager) para verificar a integridade operacional dos clusters e de seus componentes nas configurações MetroCluster over FC e MetroCluster over IP. Se os clusters estiveram envolvidos em um evento de desempenho detectado pelo Unified Manager, o status de integridade pode ajudar você a determinar se um problema de hardware ou software contribuiu para o evento.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Você deve ter analisado um evento de desempenho para uma configuração MetroCluster e obtido o nome do cluster envolvido.
- Ambos os clusters na configuração do MetroCluster por FC e IP devem ser monitorados pela mesma instância do Unified Manager.

Determine a integridade do cluster na configuração do MetroCluster sobre FC

Siga estes passos para determinar a integridade do cluster em uma configuração do MetroCluster over FC.

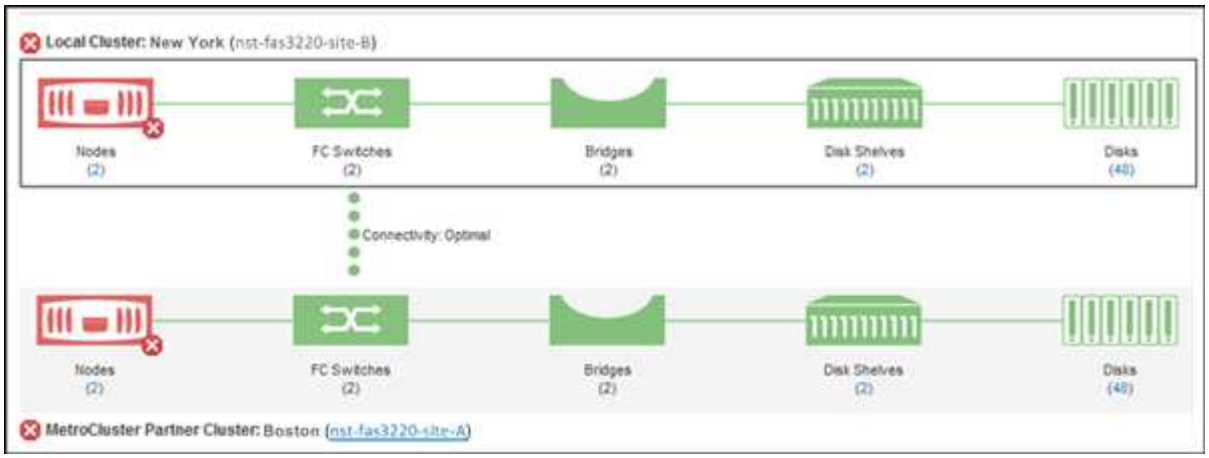
Passos

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 Origem**. Você verá todos os eventos gerados em seu ambiente para todas as configurações do MetroCluster.
3. Ao lado de um evento do MetroCluster, clique no nome do cluster.

   Caso nenhum evento do MetroCluster seja exibido, você pode usar a barra de pesquisa para procurar o nome do cluster envolvido no evento relacionado à sua configuração MetroCluster over FC.

   A visualização Saúde: todos os Clusters é exibida com informações detalhadas sobre o evento.

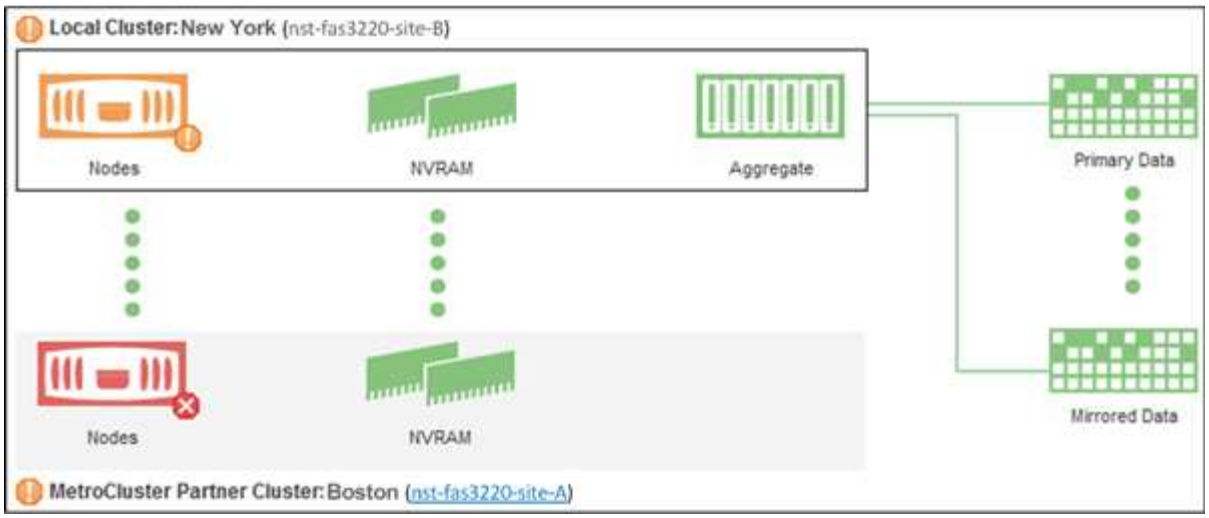
4. Selecione a guia **MetroCluster Conectividade** para exibir a integridade da conexão entre o cluster selecionado e seu cluster parceiro.



   Neste exemplo, você vê os nomes e os componentes do cluster local e do cluster parceiro. Um ícone amarelo ou vermelho indica um evento de integridade para o componente destacado. O ícone Connectivity representa a ligação 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 integridade 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 de FC Switches no cluster local ou parceiro, ou o ícone de Connectivity, estiver vermelho, um problema de integridade do link pode ter causado o evento de desempenho.

5. Selecione a guia **Replicação do MetroCluster**.



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 parceiro pode ter causado o evento de desempenho.

Determine a integridade do cluster na configuração do MetroCluster over IP

Siga estes passos para determinar a integridade do cluster em uma configuração do MetroCluster over IP.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de Eventos** para exibir a lista de eventos.
2. No painel de filtros, na categoria **Tipo de Origem**, selecione o `MetroCluster Relationship` filtro. Você vê todos os eventos gerados em seu ambiente para todas as configurações do MetroCluster.

> Caso você não consiga visualizar os eventos relatados do MetroCluster, você pode usar a barra de pesquisa para buscar pelo nome do cluster envolvido no evento relacionado à sua configuração de MetroCluster over IP.

3. Ao lado do evento relevante do MetroCluster, clique no nome do cluster. A página Clusters é exibida com os detalhes desse cluster. Para obter informações sobre como determinar problemas de integridade, consulte "Monitorar problemas de conectividade na configuração do MetroCluster sobre IP".

Visualize o status de integridade e capacidade de todos os clusters SAN Array no Active IQ Unified Manager

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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Você pode visualizar informações gerais dos clusters All SAN Array nas visualizações "Health: All Clusters" e "Capacity: All Clusters". Além disso, você pode visualizar detalhes na página "Cluster / Health details".

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Clusters**.

2. Certifique-se de que a coluna “Personality” esteja visível na visualização **Health: All Clusters** ou adicione-a usando o controle **Show / Hide**.

   Esta coluna exibe “All SAN Array” para seus clusters All SAN Array.

3. Analise as informações.
4. Para visualizar informações sobre capacidade de storage nesses clusters, selecione a visualização Capacidade: todos os clusters.
5. Para visualizar informações detalhadas sobre a integridade e capacidade de storage desses clusters, clique no nome de um cluster All SAN Array.

   Veja os detalhes nas abas Health, Capacity e Nodes na página de detalhes Cluster / Health

Visualize a lista de nós e detalhes no Active IQ Unified Manager

Você pode usar a visualização Saúde: todos os nós para ver a lista de nós em seus clusters. Você pode usar a página de detalhes de Cluster/Health para ver informações detalhadas sobre os nós que fazem parte do cluster monitorado.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Você pode visualizar detalhes como o estado do nó, o cluster que contém o nó, os detalhes da capacidade do agregado (usada e total) e os detalhes da capacidade bruta (utilizável, reserva e total). Você também pode obter informações sobre pares de HA, shelves de disco e portas.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Nós**.
2. Na visualização **Health: All Nodes**, clique no nó cujos detalhes você deseja visualizar.

   As informações detalhadas do nó selecionado são exibidas na página de detalhes Cluster / Health. O painel esquerdo exibe a lista de pares de HA. Por padrão, os Detalhes de HA ficam abertos, exibindo detalhes do estado de 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 discos	**Gavetas de disco**.
Informações relacionadas à porta	**Portas**.

Para obter mais informações, consulte:

- "Desempenho: visualização de todos os nós"
- "Visualizando os valores de IOPS disponíveis no nó e no agregado"
- "Visualizando os valores usados da capacidade de desempenho do nó e do agregado"

Gere um relatório de inventário de hardware para renovação de contrato no Active IQ Unified Manager

Você pode gerar um relatório contendo uma lista completa de informações do cluster e dos nós, como números de modelo e de série do hardware, tipos e quantidades de discos, licenças instaladas e muito mais. Este relatório é útil para a renovação de contratos em sites seguros (“dark” sites) que não estão conectados à plataforma NetAppActive IQ.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Nós**.
2. Acesse a visualização **Health: All Nodes** ou **Performance: All Nodes**.
3. Selecione **Relatórios** > ***** > Relatório de Inventário de Hardware*.

   O relatório de inventário de hardware é baixado como um arquivo .csv com informações completas até a data atual.

4. Forneça essas informações ao seu contato de suporte da NetApp para a renovação do contrato.

Visualize a lista e os detalhes das VMs de armazenamento no Active IQ Unified Manager

Na visualização "Saúde: Todas as VMs de armazenamento", você pode monitorar seu inventário de máquinas virtuais de armazenamento (SVMs). Você pode usar a página "Detalhes de VM de armazenamento/Saúde" para visualizar informações detalhadas sobre as SVMs monitoradas.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Você pode visualizar detalhes de uma SVM, como a capacidade, a eficiência e a configuração de uma SVM. Você também pode visualizar informações sobre os dispositivos relacionados e os alertas relacionados a essa SVM.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **VMs de armazenamento**.
2. Escolha uma das seguintes maneiras de visualizar os detalhes da SVM:
   - Para visualizar informações sobre a integridade de todas as SVMs em todos os clusters, no menu Exibir, selecione a exibição Integridade: todas as VMs de storage.
   - Para visualizar os detalhes completos, clique no nome da VM de armazenamento.

     Você também pode visualizar os detalhes completos clicando em **View Details** na caixa de diálogo de detalhes mínimos.

3. Visualize os objetos relacionados à SVM clicando em **View Related** 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 antirransomware"
- "Visualizando o status de segurança para clusters e VMs de armazenamento"
- "Relacionamento: visualizar todos os relacionamentos"

Veja a lista de agregados e os detalhes no Active IQ Unified Manager

Na visualização Saúde: todos os agregados, você pode monitorar seu inventário de agregados. A visualização Capacidade: todos os agregados permite que você veja informações sobre a capacidade e a utilização dos agregados em todos os clusters.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Você pode visualizar detalhes, como capacidade e configuração do agregado, além de informações de disco, na página de detalhes Aggregate / Health. Você pode usar esses detalhes antes de configurar as definições 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 do agregado:
   - Para visualizar informações sobre a integridade de todos os agregados em todos os clusters, no menu Exibir, selecione Integridade: visualização de 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 de todos os agregados.
   - Para visualizar os detalhes completos, clique no nome do agregado.

     Você também pode visualizar os detalhes completos clicando em **View Details** na caixa de diálogo de detalhes mínimos.
3. Visualize os objetos relacionados ao agregado clicando em **Exibir relacionados** na caixa de diálogo de detalhes mínimos.

Informações relacionadas

- "Página de detalhes de agregado / integridade"
- "Desempenho: visualização de todos os agregados"
- "Crie um relatório para visualizar os agregados que atingiram a capacidade máxima no Active IQ Unified Manager"

Veja as informações de capacidade do FabricPool no Active IQ Unified Manager

Você pode visualizar informações de capacidade de FabricPool para clusters, agregados e volumes nas páginas de inventário e detalhes de Capacidade e Desempenho desses objetos. Essas páginas também exibem informações de espelhamento de FabricPool

quando um nível de espelhamento tiver sido configurado.

Estas 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 conectados a uma camada de nuvem e quais volumes estão implementando os recursos do FabricPool ao mover determinadas informações para a camada de nuvem.

Quando uma camada de nuvem é espelhada para outro provedor de nuvem (a “mirror tier”), ambas as camadas de nuvem são exibidas na página de detalhes de Aggregate / Health.

Passos

1. Execute uma das seguintes ações:

Para visualizar informações sobre a capacidade de…	**Faça isso…**
Clusters	a. Na visualização Capacidade: todos os Clusters, clique em um cluster. b. Na página de detalhes Cluster / Health, clique na guia **Configuration**. A tela exibe 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 indica “SSD (FabricPool)” ou “HDD (FabricPool)”. b. Na página de detalhes de Agregado/Saúde, clique na guia **Capacidade**. A exibição mostra a capacidade total utilizada na camada de nuvem. c. Clique na aba **Informações do Disco**. A tela exibe o nome do nível de nuvem e a capacidade utilizada. d. Clique na aba **Configuração**. A tela exibe o nome do tier de nuvem e outras informações detalhadas sobre o tier de nuvem.
Volumes	a. Na visualização Capacidade: todos os Volumes, clique em um volume em que o nome de uma política aparece no campo “Política de Hierarquização”. b. Na página de detalhes de volume/saúde, clique na aba **Configuração**. A tela exibe o nome da política de hierarquização do FabricPool atribuída ao volume.

2. Na página **Workload Analysis**, você pode selecionar “Cloud Tier View” na área **Capacity Trend** para ver a capacidade usada na Performance Tier local e na Cloud Tier durante o mês anterior.

Para obter mais informações sobre os agregados do FabricPool, consulte "Visão geral de discos e agregados".

Visualize os detalhes do pool de storage no Active IQ Unified Manager

Você pode visualizar os detalhes do pool de storage para monitorar a integridade do pool de storage, o cache total e disponível e as alocações usadas e disponíveis.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Agregados**.
2. Clique no nome de um agregado.

   Você vê os detalhes do agregado selecionado.

3. Clique na aba **Informações do Disco**.

   São exibidas informações detalhadas do disco.

   A tabela Cache é exibida somente quando o agregado selecionado está usando um pool de storage.

4. Na tabela Cache, mova o ponteiro sobre o nome do pool de storage necessário.

   Os detalhes do pool de storage são exibidos.

Veja a lista de volumes e detalhes no Active IQ Unified Manager

Na visualização Saúde: todos os volumes, você pode monitorar seu inventário de volumes. A visualização Capacidade: todos os volumes permite que você veja informações sobre a capacidade e a utilização dos volumes em um cluster.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Você também pode usar a página Detalhes do Volume/Integridade para visualizar informações detalhadas sobre os volumes monitorados, incluindo a capacidade, a eficiência, a configuração e a proteção dos volumes. Você também pode visualizar informações sobre os dispositivos relacionados e os alertas associados a um volume específico.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. Escolha uma das seguintes maneiras para visualizar os detalhes do volume:
   - Para visualizar informações detalhadas sobre a integridade dos volumes em um cluster, no menu Exibir, selecione Integridade: visualização de todos os volumes.

- Para visualizar informações detalhadas sobre a capacidade e a utilização de volumes em um cluster, no menu Exibir, selecione Capacidade: visualização de todos os volumes.
- Para visualizar os detalhes completos, clique no nome do volume.

  Você também pode visualizar os detalhes completos clicando em **View Details** 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 com detalhes sobre saúde"
- "Desempenho: visualização de todos os volumes"
- "Segurança: visão antirransomware"
- "Visualizando relações de proteção de volume"
- "Criar um relatório para visualizar gráficos de capacidade de volume disponível"

Veja detalhes sobre os compartilhamentos NFS no Active IQ Unified Manager

Você pode visualizar detalhes sobre todos os compartilhamentos NFS, como seu status, o caminho associado ao volume (volumes FlexGroup ou volumes FlexVol), os níveis de acesso dos clientes aos compartilhamentos NFS e a política de exportação definida para os volumes exportados. Use a visualização "Health: All NFS Shares" para ver todos os compartilhamentos NFS em todos os clusters monitorados e use a página de detalhes "Storage VM / Health" para visualizar todos os compartilhamentos NFS em uma máquina virtual de storage (SVM) específica.

Antes de começar

- A licença NFS deve estar habilitada no cluster.
- As interfaces de rede que servem os compartilhamentos NFS devem ser configuradas.
- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Etapa

1. No painel de navegação esquerdo, siga as etapas abaixo, dependendo de você querer visualizar todos os compartilhamentos NFS ou apenas os compartilhamentos NFS de uma SVM específica.

Para…	Siga estes passos…
Veja todos os compartilhamentos NFS	Clique em **Storage** > **NFS Shares**
Visualize os compartilhamentos NFS de uma única SVM	a. Clique em **Armazenamento** > **VMs de armazenamento** b. Clique na SVM para a qual você deseja visualizar os detalhes dos compartilhamentos NFS. c. Na página de detalhes de integridade da VM de armazenamento, clique na guia **NFS Shares**.

Para obter mais informações, consulte "Provisionamento de volumes de compartilhamento de arquivos" e "Provisionamento de compartilhamentos de arquivos CIFS e NFS usando APIs".

Veja detalhes sobre compartilhamentos SMB/CIFS no Active IQ Unified Manager

Você pode visualizar detalhes sobre todos os compartilhamentos SMB/CIFS, como o nome do compartilhamento, o caminho de junção, os objetos que ele contém, as configurações de segurança e as políticas de exportação definidas para o compartilhamento. Use a visualização "Health: All SMB Shares" para ver todos os compartilhamentos SMB em todos os clusters monitorados e use a página de detalhes "Storage VM / Health" para visualizar todos os compartilhamentos SMB em uma máquina virtual de storage (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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Os compartilhamentos em pastas não são exibidos.

Etapa

1. No painel de navegação à esquerda, siga as etapas abaixo, dependendo de você querer visualizar todos os compartilhamentos SMB/CIFS ou apenas os compartilhamentos de uma SVM específica.

Para…	Siga estes passos…
Veja todos os compartilhamentos SMB/CIFS	Clique em **Storage** > **SMB Shares**
Visualize os compartilhamentos SMB/CIFS para uma única SVM	a. Clique em **Armazenamento** > **VMs de armazenamento** b. Clique na SVM para a qual você deseja visualizar os detalhes do compartilhamento SMB/CIFS. c. Na página de detalhes de integridade/VM de storage, clique na guia **Compartilhamentos SMB**.

Para obter mais informações, consulte "Provisionamento de compartilhamentos de arquivos CIFS e NFS usando APIs".

Veja a lista de cópias de Snapshot no Active IQ Unified Manager

Você pode visualizar a lista de cópias Snapshot de um volume selecionado. Você pode usar a lista de cópias Snapshot para calcular a quantidade de espaço de disco que pode ser recuperada se uma ou mais cópias Snapshot forem excluídas e pode excluir as cópias Snapshot, se necessário.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

- O volume que contém as cópias Snapshot deve estar online.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. Na visualização **Saúde: todos os volumes**, selecione o volume que contém as cópias Snapshot que você deseja visualizar.
3. Na página de detalhes de **Volume / Health**, clique na aba **Capacity**.
4. No painel **Details** da guia **Capacity**, na seção Outros detalhes, clique no link ao lado de **Snapshot Copies**.

   O número de cópias do Snapshot é um link que exibe a lista de cópias do Snapshot.

Informações relacionadas

"Página Saúde/Volumes"

Excluir cópias Snapshot no Active IQ Unified Manager

Você pode excluir uma cópia Snapshot para economizar espaço ou liberar espaço de disco, ou pode excluir a cópia Snapshot se ela não for mais necessária.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

O volume deve estar online.

Para excluir uma cópia Snapshot que esteja em uso ou bloqueada, você deve ter liberado a cópia Snapshot do aplicativo que a estava utilizando.

- Não é possível excluir a cópia Snapshot de base em um volume pai se um volume FlexClone estiver usando essa cópia Snapshot.

  A cópia Snapshot de base é a cópia Snapshot usada para criar o volume FlexClone e exibe o status `Busy` e a dependência do aplicativo como `Busy, Vclone` no volume pai.

- Não é possível excluir uma cópia Snapshot bloqueada que esteja sendo usada em uma relação do SnapMirror.

  A cópia Snapshot está bloqueada e é necessária para a próxima atualização.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. Na visualização **Saúde: todos os volumes**, selecione o volume que contém as cópias Snapshot que você deseja visualizar.

   A lista de cópias Snapshot é exibida.

3. Na página de detalhes de **Volume / Health**, clique na aba **Capacity**.
4. No painel **Details** da guia **Capacity**, na seção Outros detalhes, clique no link ao lado de **Snapshot Copies**.

O número de cópias do Snapshot é um link que exibe a lista de cópias do Snapshot.

5. Na visualização **Cópias Snapshot**, selecione as cópias Snapshot que você deseja excluir e clique em **Excluir selecionados**.

Calcule o espaço recuperável para cópias Snapshot no Active IQ Unified Manager

Você pode calcular a quantidade de espaço de disco que pode ser recuperada se uma ou mais cópias Snapshot forem excluídas.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- O volume deve estar online.
- O volume deve ser um volume FlexVol; essa funcionalidade não é compatível com volumes FlexGroup.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. Na visualização **Saúde: todos os volumes**, selecione o volume que contém as cópias Snapshot que você deseja visualizar.

   A lista de cópias Snapshot é exibida.

3. Na página de detalhes de **Volume / Health**, clique na aba **Capacity**.
4. No painel **Details** da guia **Capacity**, na seção Outros detalhes, clique no link ao lado de **Snapshot Copies**.

   O número de cópias do Snapshot é um link que exibe a lista de cópias do Snapshot.

5. Na visualização **Snapshot Copies**, selecione as cópias Snapshot para as quais você deseja calcular o espaço recuperável.
6. Clique em **Calcular**.

   O espaço recuperável (em porcentagem e em KB, MB, GB e assim por diante) no volume é exibido.

7. Para recalcular o espaço recuperável, selecione as cópias Snapshot necessárias e clique em **Recalcular**.

Compreenda as janelas e caixas de diálogo de objetos de cluster no Active IQ Unified Manager

Você pode visualizar todos os seus clusters e objetos de cluster na página do respectivo 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, saúde e desempenho do cluster
- Páginas de inventário, integridade e desempenho do agregado
- Páginas de Inventário de volume, Integridade 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 integridade do Unified Manager

Compreenda os fluxos de trabalho e tarefas comuns de saúde do Active IQ Unified Manager

Alguns fluxos de trabalho e tarefas administrativas comuns associados ao Unified Manager incluem selecionar os clusters de storage que serão monitorados; diagnosticar condições que afetam negativamente a disponibilidade de dados, a capacidade e a proteção; restaurar dados perdidos; configurar e gerenciar volumes; e agrupar e enviar dados de diagnóstico para o suporte técnico (quando necessário).

O Unified Manager permite que os administradores de storage visualizem um painel, avaliem a capacidade geral, a disponibilidade e a integridade da proteção dos clusters de storage 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, uma máquina virtual de storage (SVM), um volume ou um volume FlexGroup que afetam a capacidade de storage ou a disponibilidade de dados dos seus objetos de storage gerenciados são exibidos nos gráficos de integridade do sistema e nos eventos da página Dashboard. Quando problemas críticos são identificados, esta página fornece links para dar suporte aos fluxos de trabalho apropriados de solução de problemas.

O Unified Manager também pode ser incluído em fluxos de trabalho que incluem ferramentas de gerenciamento relacionadas, como OnCommand Workflow Automation (WFA), para oferecer suporte à configuração direta de recursos de storage.

Este documento descreve fluxos de trabalho comuns relacionados às seguintes tarefas administrativas:

- Diagnosticar e gerenciar problemas de disponibilidade

  Se uma falha de hardware ou problemas de configuração de recursos de storage causarem a exibição de eventos de disponibilidade de dados na página Painel, os administradores de storage podem seguir os links incorporados para visualizar informações de conectividade sobre o recurso de storage afetado, consultar orientações de solução de problemas e atribuir a resolução do problema a outros administradores.

- Configurando e monitorando incidentes de desempenho

  O administrador pode monitorar e gerenciar o desempenho dos recursos do sistema de storage que estão sendo monitorados. Consulte "Introdução ao monitoramento de desempenho do Active IQ Unified Manager" para obter mais informações.

- Diagnosticar e gerenciar problemas de capacidade de volume

  Se houver problemas de capacidade de storage do volume exibidos na página do Dashboard, os administradores de storage poderão seguir os links incorporados para visualizar as tendências atuais e

históricas relacionadas à capacidade de storage do volume afetado, consultar orientações de solução de problemas e atribuir a resolução do problema a outros administradores.

- Configuração, monitoramento e diagnóstico de problemas de relacionamento de proteção

  Após criar e configurar os relacionamentos de proteção, os administradores de storage podem visualizar os possíveis problemas relacionados aos relacionamentos de proteção, o estado atual dos relacionamentos de proteção, as informações atuais e históricas de sucesso do trabalho de proteção sobre os relacionamentos afetados e orientações para solução de problemas. Consulte "Aprenda sobre como gerenciar e monitorar relações de proteção" para obter mais informações.

- Criando arquivos de backup e restaurando dados de arquivos de backup.
- Associar objetos de armazenamento a anotações

  Ao associar objetos de storage a anotações, os administradores de storage podem filtrar e visualizar os eventos relacionados a esses objetos, o que permite que priorizem e resolvam os problemas associados a esses eventos.

- Utilize APIs REST para ajudar a gerenciar seus clusters, visualizando as informações de integridade, capacidade e desempenho coletadas pelo Unified Manager. Veja "Primeiros passos com as APIs REST do Active IQ Unified Manager" para obter mais informações.
- Enviar um pacote de suporte ao suporte técnico

  Os administradores de storage podem recuperar e enviar um pacote de suporte ao suporte técnico usando o console de manutenção. Os pacotes de suporte devem ser enviados ao suporte técnico quando o problema exigir um diagnóstico e uma solução de problemas mais detalhados do que o que uma mensagem AutoSupport fornece.

Monitorar e solucionar problemas de disponibilidade de dados

Monitore e solucione problemas de disponibilidade de dados no Active IQ Unified Manager

O Unified Manager monitora a confiabilidade com que os usuários autorizados podem acessar seus dados armazenados, alerta você sobre condições que bloqueiam ou impedem esse acesso e permite que você diagnostique essas condições, além de atribuir e acompanhar sua resolução.

Os tópicos de fluxo de trabalho de disponibilidade nesta seção descrevem exemplos de como um administrador de storage pode usar a interface da Web do Unified Manager para descobrir, diagnosticar e atribuir para resolução condições de hardware e software que afetam negativamente a disponibilidade de dados.

Identifique e resolva condições de link inativo da interconexão de failover de storage

Analise e resolva condições de link de interconexão de failover de armazenamento inativo no Active IQ Unified Manager

Este fluxo de trabalho fornece um exemplo de como você pode verificar, avaliar e resolver condições de link de interconexão de failover de armazenamento inativas. Neste cenário, você é um administrador que usa o Unified Manager para verificar riscos de failover de armazenamento antes de iniciar uma atualização da versão do ONTAP em seus nós.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Se as interconexões de failover de armazenamento entre os nós de um par de HA falharem durante uma tentativa de atualização sem interrupções, a atualização falhará. Portanto, a prática comum é que o administrador monitore e confirme a confiabilidade do failover de armazenamento nos nós de cluster destinados à atualização antes do início de uma atualização.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.
2. Na página de inventário **Event Management**, selecione **Active Availability events**.
3. Na parte superior da coluna **Nome** da página de inventário de **Gerenciamento de Eventos**, clique e digite `*failover` na caixa de texto para limitar a exibição a eventos relacionados ao failover de armazenamento.

   Todos os eventos passados relacionados a condições de failover de armazenamento são exibidos.

   Nesse 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 storage forem exibidos na página de inventário **Event Management**, execute as seguintes etapas:

   a. Clique no link do título do evento para exibir os detalhes desse evento.

      Neste exemplo, você clica no título do evento “Interconexão de failover de armazenamento: um ou mais links inativos”.

   A página de detalhes desse evento é exibida.

   a. Na página de detalhes do evento, você pode realizar uma ou mais das seguintes tarefas:
      - Analise a mensagem de erro no campo Cause e avalie o problema.
      - Atribua o evento a um administrador.
      - Reconheça o evento.

Informações relacionadas

"Página de detalhes do evento"

"Funções e capacidades de usuário do Unified Manager"

Execute a ação corretiva para uma falha no link de interconexão de failover de armazenamento no Active IQ Unified Manager

Ao exibir a página de detalhes 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 para o problema.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Neste cenário de exemplo, o resumo do evento fornecido na página Detalhes do evento contém as seguintes informações sobre a condição de link de interconexão de failover de armazenamento inativo:

```
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 aardvark e bonobo do par de HA está inativo, mas que o Link0 entre Apple e Boy está ativo. Como um dos links está ativo, o acesso remoto dinâmico à memória (RDMA) ainda está funcionando, e uma tarefa de failover de armazenamento ainda pode ser concluída com sucesso.

No entanto, para garantir que não haja falha em ambos os links e que a proteção de failover de armazenamento não seja totalmente desativada, você decide diagnosticar mais detalhadamente o motivo da queda do Link1.

Passos

1. Na página de detalhes de **Event**, você pode clicar no link para o evento especificado no campo Source para obter mais detalhes sobre outros eventos que possam estar relacionados à condição de queda do link de interconexão de failover de armazenamento.

   Neste exemplo, a origem do evento é o nó chamado aardvark. Clicar nesse nome de nó exibe HA Details do par de HA afetado, aardvark e bonobo, na guia Nodes da página de detalhes Cluster / Health, e exibe outros eventos que ocorreram recentemente no par de HA afetado.

2. Consulte os **Detalhes da HA** para obter mais informações sobre o evento.

   Neste exemplo, as informações relevantes estão na tabela Events. A tabela mostra o evento “Storage Failover Connection One or More Link Down”, a hora em que o evento foi gerado e, novamente, o nó de onde esse evento se originou.

Utilizando as informações de localização do nó nos Detalhes de HA, solicite ou realize pessoalmente uma inspeção física e o reparo do problema de failover de armazenamento nos nós afetados do par de HA.

Informações relacionadas

"Página de detalhes do evento"

"Funções e capacidades de usuário do Unified Manager"

Resolver problemas de volume offline

Resolva problemas de volume offline no Active IQ Unified Manager

Este fluxo de trabalho fornece um exemplo de como você pode avaliar e resolver um evento de volume off-line que o Unified Manager pode exibir na página de inventário do Event Management. Neste cenário, você é um administrador que usa o Unified Manager para solucionar problemas em um ou mais eventos de volume off-line.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Os volumes podem ser informados como off-line por vários motivos:

- O administrador do SVM colocou deliberadamente o volume off-line.
- O nó de cluster que hospeda o volume está inativo, e o failover de armazenamento para seu parceiro no par de HA também falhou.
- A máquina virtual de armazenamento (SVM) que hospeda o volume foi interrompida porque o nó que hospeda o volume raiz dessa SVM está inativo.
- O agregado que hospeda o volume está inativo devido à falha simultânea de dois discos RAID.

Você pode usar a página de inventário do Event Management e as páginas de detalhes Cluster/Health, Storage VM/Health e Volume/Health para confirmar ou eliminar uma ou mais dessas possibilidades.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.
2. Na página de inventário **Event Management**, selecione **Active Availability events**.
3. Clique no hiperlink exibido para o evento Volume Offline.

   A página de detalhes do evento referente ao incidente de disponibilidade é exibida.

4. Nessa página, verifique as observações para qualquer indicação de que o administrador da SVM tenha colocado o volume em questão off-line.
5. Na página de detalhes do **Evento**, você pode consultar as informações de uma ou mais das seguintes tarefas:
   - Analise as informações exibidas no campo "Cause" para obter possíveis orientações de diagnóstico.

     Neste exemplo, a informação no campo Causa apenas indica que o volume está off-line.

   - Verifique a área de Notas e Atualizações para ver se há alguma indicação de que o administrador do SVM tenha deliberadamente colocado o volume em questão off-line.
   - Clique na origem do evento, neste caso o volume informado como off-line, para obter mais informações sobre esse volume.
   - Atribua o evento a um administrador.
   - Confirme o evento ou, se for o caso, marque-o como resolvido.

Execute ações de diagnóstico para condições de volume offline no Active IQ Unified Manager

Após acessar a página de detalhes Volume / Saúde de um volume relatado como off-line,

você pode procurar informações adicionais úteis para diagnosticar a condição de volume off-line.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Se o volume informado como off-line não foi colocado off-line deliberadamente, esse volume pode estar off-line por vários motivos.

Na página de detalhes Volume/Integridade do volume off-line, você pode navegar para outras páginas e painéis para confirmar ou eliminar possíveis causas:

- Clique nos links da página de detalhes **Volume / Health** para determinar se o volume está off-line porque seu nó host está inativo e o failover de armazenamento para o parceiro do seu par de HA também falhou.

  Consulte "Determinar se uma condição de volume off-line é causada por um nó inativo".

- Clique nos links da página de detalhes **Volume / Health** para determinar se o volume está off-line e se a máquina virtual de armazenamento (SVM) do host está parada porque o nó que hospeda o volume raiz dessa SVM está inativo.

  Consulte "Determinar se um volume está off-line e se a SVM está parada porque um nó está inativo".

- Clique nos links da página de detalhes **Volume / Health** para determinar se o volume está off-line devido a discos com falha no agregado host.

  Consulte "Determinar se um volume está off-line devido a discos com falha em um agregado".

Informações relacionadas

"Funções e capacidades de usuário do Unified Manager"

Determine se um volume está offline porque seu nó host está inativo no Active IQ Unified Manager

Você pode usar a interface da web do Unified Manager para confirmar ou descartar a possibilidade de um volume estar off-line porque seu nó host está inativo e o failover de armazenamento para o nó parceiro em seu par de HA não foi bem-sucedido.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Para determinar se a condição de volume off-line é causada por falha no nó de hospedagem e pelo failover de armazenamento malsucedido subsequente, execute as seguintes ações:

Passos

1. Localize e clique no link de hipertexto exibido sob SVM no painel **Dispositivos Relacionados** da página de detalhes **Volume / Integridade** do volume off-line.

   A página Detalhes da VM de armazenamento/Integridade exibe informações sobre a máquina virtual de armazenamento (SVM) que hospeda o volume off-line.

2. No painel **Dispositivos Relacionados** da página de detalhes **VM de armazenamento / integridade**, localize e clique no link de hipertexto exibido em Volumes.

A visualização "Health: All Volumes" exibe uma tabela com informações sobre todos os volumes hospedados pela SVM.

3. No cabeçalho da coluna Estado da visualização **Saúde: Todos os Volumes**, clique no símbolo de filtro e selecione a opção **Offline**.

   Somente os volumes da SVM que estão em estado off-line são listados.

4. Na visualização Saúde: todos os volumes, clique no símbolo de grade e, em seguida, selecione a opção **Nós do cluster**.

   Você pode precisar rolar na caixa de seleção da grade para localizar a opção **Nós do Cluster**.

   A coluna "Nós do Cluster" foi adicionada ao inventário de volumes e exibe o nome do nó que hospeda cada volume off-line.

5. Na visualização **Health: All Volumes**, localize a entrada do volume off-line e, na coluna Cluster Node, clique no nome do nó que o hospeda.

   A aba Nodes na página de detalhes Cluster / Health exibe o estado do par de HA de nós ao qual o nó host pertence. O estado do nó host e o êxito de qualquer operação de failover de clusters são indicados na exibição.

Após confirmar que a condição de volume off-line existe porque o nó do host está inativo e o failover de armazenamento para o nó parceiro do par de HA falhou, entre em contato com o administrador ou operador responsável para reiniciar manualmente o nó inativo e corrigir o problema de failover de armazenamento.

Determine se um volume está offline porque seu SVM foi interrompido no Active IQ Unified Manager

Você pode usar a interface do usuário da web do Unified Manager para confirmar ou descartar a possibilidade de um volume estar off-line porque a máquina virtual de armazenamento (SVM) host foi interrompida devido à inatividade do nó que hospeda o volume raiz dessa SVM.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Para determinar se a condição de volume off-line é causada pela interrupção da SVM hospedeira porque o nó que hospeda o volume raiz dessa SVM está inativo, execute as seguintes ações:

Passos

1. Localize e clique no link de hipertexto exibido abaixo da SVM no painel **Dispositivos relacionados** da página de detalhes **Volume / Integridade** do volume off-line.

   A página de detalhes de integridade da VM de armazenamento exibe o status “running” ou “stopped” da SVM que a hospeda. Se o status da SVM for `running`, a condição de volume off-line não será causada pela indisponibilidade do nó que hospeda o volume raiz dessa SVM.

2. Se o status da SVM estiver stopped, clique em **View SVMs** para identificar melhor a causa de a SVM hospedeira estar parada.
3. Na visualização **Saúde: todas as VMs de armazenamento** no cabeçalho da coluna SVM clique no símbolo de filtro e digite o nome da SVM parada.

As informações dessa SVM são mostradas em uma tabela.

4. Na visualização **Saúde: Todas as VMs de armazenamento**, clique  e depois selecione a opção **Volume raiz**.

   A coluna Volume raiz é adicionada ao inventário da SVM e exibe o nome do volume raiz da SVM interrompida.

5. Na coluna Root Volume, clique no nome do volume raiz para exibir a página de detalhes **Storage VM / Health** desse volume.

   Se o status do volume raiz da SVM for (Online), então a condição original de volume off-line não é causada pelo fato de o nó que hospeda o volume raiz dessa SVM estar inativo.

6. Se o status do volume raiz da SVM for (Offline), localize e clique no link de hipertexto exibido em Agregado no painel Dispositivos Relacionados da página de detalhes Volume/Integridade do volume raiz da SVM.
7. Localize e clique no link de hipertexto exibido sob Nó no painel **Dispositivos Relacionados** da página de detalhes **Agregado / Saúde** do agregado.

   A guia Nós na página de detalhes Cluster / Health exibe o estado do par de HA de nós ao qual pertence o nó que hospeda o volume raiz da SVM. O estado do nó é indicado na tela.

Depois que você confirmar que a condição de volume off-line é causada pela condição off-line da SVM host desse volume, que por sua vez é causada porque o nó que hospeda o volume raiz dessa SVM está inativo, entre em contato com o administrador ou operador apropriado para reiniciar manualmente o nó inativo.

Determine se um volume está offline devido a discos defeituosos no Active IQ Unified Manager

Você pode usar a interface do usuário da Web do Unified Manager para confirmar ou descartar a possibilidade de que um volume esteja off-line porque problemas de disco RAID colocaram seu agregado host off-line.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Para determinar se a condição de volume off-line é causada por problemas de disco RAID que estão colocando o agregado de hospedagem off-line, execute as seguintes ações:

Passos

1. Localize e clique no link de hipertexto exibido em Aggregate no painel **Related Devices** da página de detalhes **Volume / Health**.

   A página Detalhes do Agregado/Saúde exibe o status online ou off-line do agregado de hospedagem. Se o status do agregado for online, os problemas de disco RAID não serão a causa de o volume estar off-line.

2. Se o status do agregado estiver off-line, clique em **Informações do disco** e procure eventos de disco corrompido na lista **Eventos** na guia **Informações do disco**.
3. Para identificar melhor os discos defeituosos, clique no hiperlink exibido em Nó no painel **Dispositivos Relacionados**.

   A página de detalhes de Cluster / Health é exibida.

4. Clique em **Discos** e selecione **Com defeito** no painel **Filtros** para listar todos os discos no estado com defeito.

   Se os discos em estado defeituoso causaram o estado off-line do agregado de host, o nome do agregado será exibido na coluna "Impacted Aggregate".

Após confirmar que a condição de volume off-line é causada por discos RAID defeituosos e pelo consequente agregado de host off-line, entre em contato com o administrador ou operador responsável para substituir manualmente os discos defeituosos e colocar o agregado on-line novamente.

Resolver problemas de capacidade

Resolva problemas de capacidade no Active IQ Unified Manager

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 apresenta problemas de capacidade. Você deseja determinar a possível causa e a solução para o problema.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Na página Dashboard, procure um evento de erro “Volume Space Full” no painel Capacity, na lista suspensa events.

Passos

1. No painel **Capacity** da página **Dashboard**, clique no nome do evento de erro Volume Space Full.

   A página de detalhes do evento referente ao erro é exibida.

2. Na página de detalhes do **Event**, você pode realizar uma ou mais das seguintes tarefas:
   - Analise a mensagem de erro no campo Causa e clique nas sugestões em Ações Corretivas Sugeridas para consultar as descrições das possíveis soluções.
   - Clique no nome do objeto, neste caso um volume, no campo Source para obter detalhes sobre o objeto.
   - Procure anotações que possam ter sido adicionadas sobre este evento.
   - Adicione uma nota ao evento.
   - Atribua 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 completo no Active IQ Unified Manager

Após receber um evento de erro “Volume Space Full”, você revisa as ações corretivas

sugeridas na página de detalhes do evento e decide executar uma das ações sugeridas.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

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 "Espaço de volume cheio" na página de inventário do Unified ManagerEvent Management e clicou no nome do evento.

As possíveis ações corretivas que você pode realizar para um volume cheio incluem o seguinte:

- Habilitar o crescimento automático, a deduplicação ou a compressão 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 na ONTAP CLI, você pode usar o Unified Manager para encontrar informações de que talvez precise para determinar quais ações tomar.

Passos

1. Na página de detalhes do **Evento**, clique no nome do volume no campo Origem para visualizar os detalhes sobre o volume afetado.
2. Na página de detalhes **Volume / Saúde**, você clica em **Configuração** e vê que a deduplicação e a compressão já estão ativadas no volume.

   Você decide redimensionar o volume.

3. No painel **Dispositivos Relacionados**, clique no nome do agregado de hospedagem para verificar se ele pode acomodar um volume maior.
4. Na página de detalhes **Aggregate / Health**, você vê que o agregado que hospeda o volume cheio 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 integridade

Saiba mais sobre os limites de integridade da capacidade de storage no Active IQ Unified Manager

Um limite de integridade da capacidade de storage é o ponto em que o servidor do Unified Manager gera eventos para relatar qualquer problema de capacidade com objetos de storage. Você pode configurar alertas para enviar notificações sempre que esses eventos ocorrerem.

Os limites de integridade da capacidade de storage para todos os agregados, volumes e qtrees estão definidos com os valores padrão. Você pode alterar as configurações conforme necessário para um objeto ou um grupo de objetos.

Configure as configurações globais de limite de integridade

Configure as definições de limite de integridade global no Active IQ Unified Manager

Você pode configurar condições globais de limite de integridade para capacidade, crescimento, reserva do Snapshot, cotas e inodes para monitorar com eficácia o tamanho do seu agregado, volume e qtree. Você também pode editar as configurações para gerar eventos quando os limites de atraso forem excedidos.

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 os alertas estiverem configurados, uma notificação de alerta é enviada. Os limites padrão são definidos com os valores recomendados, mas você pode modificá-los para gerar eventos em intervalos que atendam às suas necessidades específicas. Quando os limites são alterados, os eventos são gerados ou se tornam obsoletos no próximo ciclo de monitoramento.

As configurações globais de limite de saúde podem ser acessadas na seção Limites de Evento 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 informações, consulte "Configurando valores globais de limite de integridade do agregado".

  Você pode configurar as definições de limite de integridade para capacidade, crescimento e cópias Snapshot de todos os agregados para monitorar qualquer violação de limite.

- Para informações, consulte "Configurando os valores globais de limite de integridade de volume".

  Você pode editar as configurações de limite de integridade para capacidade, cópias Snapshot, cotas de qtree, crescimento do volume, espaço da reserva de substituição e inodes para todos os volumes, a fim de monitorar qualquer violação de limite.

- Para informações, consulte "Configurando os valores de limite de integridade global do qtree".

  Você pode editar as configurações de limite de integridade para a capacidade de todas as qtrees para monitorar qualquer violação desse limite.

- Para informações, consulte "Editar as configurações de limite de integridade de atraso para relacionamentos de proteção não gerenciados".

  Você pode aumentar ou diminuir a porcentagem do tempo de atraso de aviso ou erro para que os eventos sejam gerados em intervalos mais adequados às suas necessidades.

Configure os valores globais de limite de integridade de agregados no Active IQ Unified Manager

Você pode configurar valores globais de limite de integridade para todos os agregados a fim de monitorar qualquer violação de limite. Eventos apropriados são gerados para violações de limite e você pode tomar medidas preventivas com base nesses eventos. Você pode configurar os valores globais com base nas configurações de melhores práticas para limites que se aplicam a todos os agregados monitorados.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Ao configurar as opções globalmente, os valores padrão dos objetos são modificados. No entanto, se os valores padrão tiverem sido alterados no nível do objeto, os valores globais não serão modificados.

As opções de limite têm valores padrão para melhor monitoramento, no entanto, você pode alterar os valores para atender aos requisitos do seu ambiente.

Quando o Autogrow está ativado em volumes que residem no agregado, os limites de capacidade do agregado são considerados ultrapassados com base no tamanho máximo do volume definido pelo Autogrow, e não com base no tamanho original do volume.

Os valores de limite de integridade não se aplicam ao agregado de raiz do nó.

Passos

1. No painel de navegação à esquerda, clique em **Limiares de eventos** > **Agregado**.
2. Configure os valores de limite apropriados para capacidade, crescimento e cópias Snapshot.
3. Clique em **Salvar**.

Informações relacionadas

"Adicionando usuários"

Configure os valores de limite de integridade do volume global no Active IQ Unified Manager

Você pode configurar os valores globais de limite de integridade para todos os volumes a fim de monitorar qualquer violação de limite. Eventos apropriados são gerados para violações dos limites de integridade, e você pode tomar medidas preventivas com base nesses eventos. Você pode configurar os valores globais com base nas configurações de melhores práticas para limites que se aplicam a todos os volumes monitorados.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

A maioria das opções de limite possui valores padrão para melhor monitoramento. No entanto, você pode alterar os valores para adequá-los às necessidades do seu ambiente.

Observe que, quando o Autogrow está ativado em um volume, os limites de capacidade são considerados ultrapassados com base no tamanho máximo do volume definido pelo Autogrow, e não com base no tamanho original do volume.

O valor padrão de 1000 cópias Snapshot se aplica apenas 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 Snapshot por volume. Para essas versões mais antigas, o Unified Manager interpreta esse número, 1000, e qualquer número entre 1000 e 250, como 250; isso significa que você continuará recebendo eventos quando o número de cópias Snapshot atingir 250. Se você quiser definir esse limite para menos de 250 nessas versões mais antigas, deverá defini-lo como 250 ou menos aqui, na visualização Health: All Volumes, ou na página de detalhes Volume / Health.

Passos

1. No painel de navegação esquerdo, clique em **Limiares de Evento** > **Volume**.

2. Configure os valores de limite apropriados para capacidade, cópias Snapshot, cotas de qtree, crescimento de volume e inodes.
3. Clique em **Salvar**.

Informações relacionadas

"Adicionando usuários"

Configure os valores de limite de integridade global do qtree no Active IQ Unified Manager

Você pode configurar os valores globais de limite de integridade para todas as qtrees para monitorar qualquer violação de limite. Eventos apropriados são gerados para violações de limite de integridade, e você pode tomar medidas preventivas com base nesses eventos. Você pode configurar os valores globais com base nas configurações de melhores práticas para limites que se aplicam a todas as qtrees monitoradas.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

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 foi definida na qtree. Os eventos não são 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 **Limiares de eventos** > **Qtree**.
2. Configure os valores de limite de capacidade apropriados.
3. Clique em **Salvar**.

Configure os limites de atraso para relacionamentos de proteção não gerenciados no Active IQ Unified Manager

Você pode editar as configurações globais padrão dos limites de integridade de aviso e erro de atraso para relacionamentos de proteção não gerenciados, de forma que os eventos sejam gerados em intervalos adequados às suas necessidades.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

O tempo de atraso não deve ser superior ao intervalo definido da programação de transferência. Por exemplo, se a programação de transferência for de hora em hora, o tempo de atraso não deve ser superior a uma hora. O limite de atraso especifica uma porcentagem que o tempo de atraso não deve exceder. Usando o exemplo de uma hora, se o limite de atraso for definido como 150%, você receberá um evento quando o tempo de atraso for superior a 1,5 horas.

As configurações descritas nesta tarefa são aplicadas globalmente a todos os relacionamentos de proteção não gerenciados. As configurações não podem ser especificadas e aplicadas exclusivamente a um relacionamento de proteção não gerenciado.

Passos

1. No painel de navegação esquerdo, clique em **Limiares de Evento** > **Relacionamento**.
2. Aumente ou diminua a porcentagem global padrão do tempo de atraso para avisos ou erros, conforme necessário.
3. Para impedir que um aviso ou evento de erro seja acionado por qualquer valor de limite de atraso, desmarque a caixa ao lado de **Enabled**.
4. Clique em **Salvar**.

Informações relacionadas

"Adicionando usuários"

Edite as configurações individuais de limite de integridade de agregado no Active IQ Unified Manager

Você pode editar as configurações de limite de integridade para a capacidade, o crescimento e as cópias de Snapshot 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 precisa ter a função de Application Administrator ou Storage Administrator.

Com base nas alterações nos valores de limite, os eventos são gerados ou ficam obsoletos no próximo ciclo de monitoramento.

Quando o Autogrow está ativado em volumes que residem no agregado, os limites de capacidade do agregado são considerados ultrapassados com base no tamanho máximo do volume definido pelo Autogrow, e não com base no tamanho original do volume.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Agregados**.
2. Na visualização **Health: All Aggregates**, selecione um ou mais agregados e clique em **Edit Thresholds**.
3. Na caixa de diálogo **Edit Aggregate Thresholds**, edite as configurações de limite de um dos seguintes itens: capacidade, crescimento ou cópias Snapshot, selecionando a caixa de seleção apropriada e, em seguida, modificando as configurações.
4. Clique em **Salvar**.

Informações relacionadas

"Adicionando usuários"

Edite as configurações individuais de limite de integridade do volume no Active IQ Unified Manager

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 precisa ter a função de Application Administrator ou Storage Administrator.

Com base nas alterações nos valores de limite, os eventos são gerados ou ficam obsoletos no próximo ciclo de monitoramento.

Observe que, quando o Autogrow está ativado em um volume, os limites de capacidade são considerados ultrapassados com base no tamanho máximo do volume definido pelo Autogrow, e não com base no tamanho original do volume.

> O valor padrão de 1000 cópias Snapshot se aplica apenas 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 Snapshot por volume. Para essas versões mais antigas, o Unified Manager interpreta esse número, 1000, e qualquer número entre 1000 e 250, como 250; isso significa que você continuará recebendo eventos quando o número de cópias Snapshot atingir 250. Se você quiser definir esse limite para menos de 250 nessas versões mais antigas, deverá defini-lo como 250 ou menos aqui, na visualização Health: All Volumes, ou na página de detalhes Volume / Health.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. Na visualização **Saúde: todos os volumes**, selecione um ou mais volumes e clique em **Editar limiares**.
3. Na caixa de diálogo **Edit Volume Thresholds**, edite as configurações de limite de um dos seguintes itens: capacidade, cópias Snapshot, cota de qtree, crescimento ou inodes selecionando a caixa de seleção apropriada e, em seguida, modificando as configurações.
4. Clique em **Salvar**.

Informações relacionadas

"Adicionando usuários"

Edite as configurações individuais de limite de integridade do qtree no Active IQ Unified Manager

Você pode editar as configurações de limite de integridade da 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 precisa ter a função de Application Administrator ou Storage Administrator.

Com base nas alterações nos valores de limite, os eventos são gerados ou ficam 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 limiares**.
3. Na caixa de diálogo **Editar Limiares de qtree**, altere os limiares de capacidade para a qtree ou as qtrees selecionadas e clique em **Salvar**.

> Você também pode definir limites individuais de qtree para qtrees na guia Qtrees da página

de detalhes de integridade da VM de armazenamento.

Gerenciar objetivos de segurança do cluster

Gerencie os objetivos de segurança do cluster no Active IQ Unified Manager

O Unified Manager fornece um painel que identifica o nível de segurança dos seus clusters do ONTAP, máquinas virtuais de storage (SVMs) e volumes, com base nas recomendações definidas no *NetApp Security Hardening Guide for ONTAP 9*.

O objetivo do painel de segurança é mostrar quaisquer áreas em que seus clusters ONTAP não estejam em conformidade 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 a ONTAP CLI. Sua organização pode não seguir todas as recomendações, portanto, em alguns casos, você não precisará fazer nenhuma alteração.

Consulte o "NetApp Guia de Reforço de Segurança para o ONTAP 9" (TR-4569) para obter recomendações e resoluções detalhadas.

Além de reportar o status de segurança, o Unified Manager também gera eventos de segurança para qualquer cluster ou SVM que apresente violações de segurança. Você pode acompanhar esses problemas na página de inventário do Event Management e configurar alertas para que o seu administrador de storage seja notificado quando novos eventos de segurança ocorrerem.

Para obter mais informações, consulte "Quais critérios de segurança estão sendo avaliados".

Quais critérios de segurança estão sendo avaliados

Entenda como o Active IQ Unified Manager avalia os critérios de segurança

Em geral, os critérios de segurança para seus clusters do ONTAP, máquinas virtuais de storage (SVMs) e volumes são avaliados em relação às recomendações definidas no *NetApp Security Hardening Guide for ONTAP 9*.

Algumas das verificações de segurança incluem:

- se um cluster está usando um método de autenticação seguro, como SAML
- se os clusters interligados têm sua comunicação criptografada
- se uma máquina virtual de storage tem seu log de auditoria ativado
- se seus volumes têm criptografia de software ou de hardware ativada

Consulte os tópicos sobre categorias de conformidade e o "NetApp Guia de Reforço de Segurança para o ONTAP 9" para obter informações detalhadas.

> Os eventos de upgrade relatados pela plataforma do 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 obter mais informações, consulte "Gerenciar os objetivos de segurança do cluster".

Compreenda as categorias de conformidade de cluster no Active IQ Unified Manager

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 se o cluster está em conformidade ou não.

Ter SVMs não conformes em um cluster afetará o valor de conformidade do cluster. Portanto, em alguns casos, pode ser necessário corrigir um problema de segurança em uma SVM antes que a segurança do cluster seja considerada em conformidade.

Observe que nem todos os parâmetros listados abaixo aparecem em todas as instalações. Por exemplo, se você não tiver clusters emparelhados ou se tiver desativado o AutoSupport em um cluster, não verá os itens "Emparelhamento de Cluster" ou "AutoSupport HTTPS Transport" na página da interface de usuário.

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
FIPS global	Indica se o modo de conformidade Global FIPS (Federal Information Processing Standard) 140-2 está ativado ou desativado. Quando o FIPS está ativado, o TLSv1 e o SSLv3 são desativados, e somente o TLSv1.1 e o TLSv1.2 são permitidos.	Habilitado	Sim
Telnet	Indica se o acesso Telnet ao sistema está habilitado ou desabilitado. 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
Banner de login	Indica se o banner de login está habilitado ou desabilitado para os usuários que acessam o sistema.	Habilitado	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
Interconexão de clusters	Indica se a comunicação entre clusters emparelhados é criptografada ou não criptografada. A criptografia deve estar configurada nos clusters de origem e de destino para que este parâmetro seja considerado em conformidade.	Criptografado	Sim
Protocolo de Tempo de Rede	Indica se o cluster possui 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 Online Certificate Status Protocol (OCSP) no nível da máquina virtual de armazenamento (SVM, anteriormente conhecida como Vserver). Isso significa que a validação de OCSP é aplicada a todas as conexões SSL/TLS feitas com a SVM e garante a integridade e a validade dos certificados usados nessas conexões.	Habilitado	Não
Log de auditoria remoto	Indica se o encaminhamento de logs (Syslog) está criptografado ou não criptografado.	Criptografado	Sim
AutoSupport Transporte HTTPS	Indica se o HTTPS é usado como protocolo de transporte padrão para enviar mensagens do AutoSupport ao suporte da NetApp.	Habilitado	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
Usuário administrador padrão	Indica se o usuário administrador padrão (incorporado) está ativado ou desativado. NetApp recomenda bloquear (desativar) todas as contas incorporadas desnecessárias.	Desabilitado	Sim
Usuários SAML	Indica se o SAML está configurado. O SAML permite que você configure a autenticação multifator (MFA) como método de login para single sign-on.	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, em comparação com usuários locais.	Não	Não
Usuários de certificado	Indica se um usuário com certificado está configurado para fazer login no cluster.	Não	Não
Usuários locais	Indica se os usuários locais estão configurados para fazer login no cluster.	Não	Não
Shell remoto	Indica se o RSH está habilitado. Por motivos de segurança, o RSH deve ser desabilitado. O Secure Shell (SSH) para acesso remoto seguro é o método preferencial.	Desabilitado	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
MD5 em uso	Indica se as contas de usuário do ONTAP usam a função de hash MD5, menos segura. A migração das contas de usuário com hash MD5 para uma função de hash criptográfica mais segura, como SHA-512, é recomendada.	Não	Sim
Tipo de emissor do certificado	Indica o tipo de certificado digital utilizado.	Assinado pela CA	Não

Entenda as categorias de conformidade de VMs de armazenamento no Active IQ Unified Manager

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 a SVM estar em conformidade ou não.

Parâmetro	Descrição	Recomendação	Afeta o SVM Compliance
Registro de auditoria	Indica se o registro de auditoria está ativado ou desativado.	Habilitado	Sim
Configurações SSH inseguras	Indica se o SSH usa cifras inseguras, por exemplo cifras que começam com `cbc*`.	Não	Sim
Banner de login	Indica se o banner de login está habilitado ou desabilitado para usuários que acessam SVMs no sistema.	Habilitado	Sim
Criptografia LDAP	Indica se a criptografia LDAP está ativada ou desativada.	Habilitado	Não
Autenticação NTLM	Indica se a autenticação NTLM está ativada ou desativada.	Habilitado	Não
Assinatura de carga útil LDAP	Indica se a assinatura de payload LDAP está ativada ou desativada.	Habilitado	Não
Configurações CHAP	Indica se o CHAP está ativado ou desativado.	Habilitado	Não
Kerberos V5	Indica se a autenticação Kerberos V5 está ativada ou desativada.	Habilitado	Não

Parâmetro	Descrição	Recomendação	Afeta o SVM Compliance
Autenticação NIS	Indica se o uso da autenticação NIS está configurado.	Desabilitado	Não
Status ativo do FPolicy	Indica se a FPolicy foi criada ou não.	Sim	Não
Criptografia SMB ativada	Indica se o SMB -Signing & Sealing não está ativado.	Sim	Não
Assinatura SMB ativada	Indica se o SMB -Signing não está habilitado.	Sim	Não

Entenda as categorias de conformidade de volume no Active IQ Unified Manager

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 o acesso de usuários não autorizados.

Observe que os parâmetros de criptografia do volume não afetam se o cluster ou a máquina virtual de armazenamento é considerado compatível.

Parâmetro	Descrição
Criptografado por software	Exibe o número de volumes protegidos usando as soluções de criptografia por software NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
Criptografado por hardware	Exibe o número de volumes protegidos usando a criptografia de hardware NetApp Storage Encryption (NSE).
Criptografia de software e hardware	Exibe o número de volumes protegidos por criptografia de software e de hardware.
Não criptografado	Exibe o número de volumes que não estão criptografados.

Saiba mais sobre o status de conformidade do cluster e do SVM no Active IQ Unified Manager

Clusters e máquinas virtuais de armazenamento (SVMs) são considerados não conformes quando qualquer um dos critérios de segurança avaliados em relação às recomendações definidas no *Guia de Reforço de Segurança da NetApp para ONTAP 9* não for atendido. Além disso, um cluster é considerado não conforme quando qualquer SVM for sinalizada como não conforme.

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 de criptografia do volume não contribui para determinar se o cluster ou a SVM são considerados em conformidade.

Visualize o status de segurança de clusters e VMs de armazenamento no Active IQ Unified Manager

O Active IQ Unified Manager permite visualizar o status de segurança dos objetos de armazenamento no seu ambiente a partir de diferentes pontos da interface. Você pode coletar e analisar informações e relatórios com base em parâmetros definidos e detectar comportamentos suspeitos ou alterações não autorizadas no sistema em clusters e máquinas virtuais de storage monitorados.

Para obter recomendações de segurança, consulte o "NetApp Guia de Reforço de Segurança para o ONTAP 9"

Veja o status da segurança em nível de objeto na página Segurança

Como administrador do sistema, você pode usar a página **Segurança** para ter visibilidade da robustez da segurança dos seus clusters do ONTAP e VMs de storage nos níveis de data center e site. Os objetos suportados são cluster, VMs de storage e volumes. Siga estes passos:

Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Dependendo de você querer 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 **Security**. A página Security é exibida.

Clicar nos gráficos de barras, contagens e `View Reports` links leva você à página de Volumes, Clusters ou Storage VMs, onde você pode visualizar os detalhes correspondentes ou gerar relatórios, conforme necessário.

A página de Segurança exibe os seguintes painéis:

- **Conformidade do cluster**: o status de segurança (número de clusters que estão em conformidade ou fora de conformidade) de todos os clusters em um data center
- **Conformidade de VMs de armazenamento**: o status de segurança (número de VMs de armazenamento que estão em conformidade ou não estão em conformidade) para todas as VMs de armazenamento no seu data center
- **Criptografia de volume**: o status da criptografia de todos os volumes no seu ambiente (número de volumes criptografados ou não criptografados)
- **Status de anti-ransomware do volume**: 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 que usam 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 **Storage > Clusters**.
2. Selecione **Exibir > Segurança > Todos os clusters**.

São exibidos os parâmetros de segurança padrão, como FIPS global, Telnet, configurações inseguras de SSH, banner de login, protocolo de tempo de rede, transporte HTTPS do AutoSupport e o status de expiração do certificado do cluster.

Você pode clicar no botão "mais opções" e escolher visualizar os detalhes de segurança na página **Security** do Unified Manager ou no System Manager. Você precisa ter credenciais válidas para visualizar os detalhes no System Manager.

Se um cluster tiver um certificado expirado, você pode clicar `expired` em **Validade do Certificado do Cluster** e renová-lo no System Manager (9.10.1 e posterior). Não é possível clicar `expired` se a instância do System Manager for de uma versão anterior à 9.10.1.

Veja os detalhes de segurança de todos os clusters na página de VMs de storage

A página de detalhes **VMs de armazenamento / Segurança** permite que você visualize o status de conformidade de segurança no nível de uma VM de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > VMs de storage**.
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 storage verificando os parâmetros de segurança, como VMs de storage, cluster, banner de login, log de auditoria e configurações de SSH inseguras.

Você pode clicar no botão "mais opções" e escolher visualizar os detalhes de segurança na página **Security** do Unified Manager ou no System Manager. Você precisa ter credenciais válidas para visualizar os detalhes no System Manager.

Para obter detalhes de segurança anti-ransomware para volumes e VMs de storage, consulte "Visualizando o status do anti-ransomware de todos os volumes e VMs de storage".

Visualize eventos de segurança que podem exigir atualizações de software ou firmware no Active IQ Unified Manager

Existem determinados eventos de segurança que têm como área de impacto “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 precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Você pode querer tomar medidas corretivas imediatas para alguns desses problemas, enquanto outros podem esperar até a próxima manutenção programada. Você pode visualizar todos esses eventos e atribuí-los aos 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 você a identificá-los para que

você possa desativá-los.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.

   Por padrão, todos os eventos ativos (novos e confirmados) são exibidos na página de inventário do Gerenciamento de Eventos.

2. No menu Exibir, selecione **Eventos de atualização**.

   A página exibe todos os eventos de segurança de atualização ativos.

Veja como os clusters gerenciam a autenticação em todos os clusters no Active IQ Unified Manager

A página Security exibe os tipos de autenticação usados para autenticar usuários em cada cluster e o número de usuários que acessam o cluster usando cada tipo. Isso permite que você verifique se a autenticação está sendo realizada de forma segura, conforme definido pela sua organização.

Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Na parte superior do painel de controle, selecione **Todos os Clusters** no menu suspenso.
3. Clique na seta para a direita no painel **Segurança** e a página **Segurança** é exibida.
4. Consulte o cartão **Cluster Authentication** para ver o número de usuários que acessam o sistema usando cada tipo de autenticação.
5. Consulte o cartão **Segurança do Cluster** para ver os mecanismos de autenticação usados para autenticar usuários em cada cluster.

Se houver usuários acessando o sistema por meio de um método inseguro ou de um método não recomendado pela NetApp, você pode desativar esse método.

Veja o status de criptografia de todos os volumes no Active IQ Unified Manager

Você pode visualizar uma lista de todos os volumes e seus respectivos status atuais de criptografia para determinar se os dados em seus volumes estão adequadamente protegidos contra o acesso por usuários não autorizados.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Os tipos de criptografia que podem ser aplicados a um volume são:

- Software: volumes protegidos usando as soluções de criptografia de software NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
- Hardware: volumes protegidos usando criptografia de hardware do NetApp Storage Encryption (NSE).
- Software e hardware: volumes protegidos por criptografia de software e de hardware.
- Nenhum: volumes que não estão criptografados.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Saúde** > **Criptografia de volumes**
3. Na visualização **Health: Volumes Encryption**, classifique pelo campo **Encryption Type** ou use o filtro para exibir volumes que tenham um tipo de criptografia específico ou que não estejam criptografados (**Encryption Type** de “None”).

Visualize o status de proteção contra ransomware de todos os volumes e máquinas virtuais de armazenamento no Active IQ Unified Manager

Você pode visualizar uma lista de todos os volumes e máquinas virtuais de storage (SVMs) e seu status atual contra ransomware, para determinar se os dados em seus volumes e SVMs estão adequadamente protegidos contra ataques de ransomware.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Para obter mais informações sobre os diferentes status de anti-ransomware, consulte "O ONTAP: ativar a proteção contra ransomware".

Visualize os detalhes de segurança de todos os volumes com detecção anti-ransomware

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Integridade** > **Segurança** > **Anti-ransomware**
3. Na visualização **Segurança: anti-ransomware**, você pode ordenar pelos vários campos ou usar o filtro.

> A proteção contra ransomware não é compatível com volumes offline, volumes restritos, volumes SnapLock, volumes FlexGroup, volumes FlexCache, volumes somente SAN, volumes de VMs de storage interrompidas, volumes raiz de VMs de storage ou volumes de proteção de dados.

Visualize os 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 storage**.
2. Selecione **Exibir > Segurança > Antiransomware**. Uma lista de SVMs com o status de antiransomware é exibida.

> O monitoramento anti-ransomware não é suportado em máquinas virtuais de storage que não têm o protocolo NAS ativado.

Visualize todos os eventos de segurança ativos no Active IQ Unified Manager

Você pode visualizar todos os eventos de segurança ativos e, em seguida, atribuir cada um deles a um usuário que possa resolver o problema. Além disso, se houver determinados eventos de segurança que você não deseja receber, esta lista pode ajudar você a identificar os eventos que deseja desativar.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.

   Por padrão, os eventos Novos e Reconhecidos são exibidos na página de inventário de gerenciamento de eventos.

2. No menu Exibir, selecione **eventos de segurança ativos**.

   A página exibe todos os eventos de segurança novos e reconhecidos gerados nos últimos 7 dias.

Adicione alertas para eventos de segurança no Active IQ Unified Manager

Você pode configurar alertas para eventos de segurança individuais, assim como para qualquer outro evento recebido pelo Unified Manager. Além disso, se desejar tratar todos os eventos de segurança da mesma forma e enviar e-mails para a mesma pessoa, você pode criar um único alerta para que você seja notificado quando qualquer evento de segurança for acionado.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

O exemplo abaixo mostra como criar um alerta para o evento de segurança “Telnet Protocol Enabled”. Isso enviará um alerta se o acesso Telnet estiver configurado para acesso administrativo remoto no cluster. Você pode usar essa mesma metodologia para criar alertas para todos os eventos de segurança.

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
2. Na página **Alert Setup**, clique em **Add**.
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 o cluster no qual você deseja ativar este alerta.
5. Clique em **Eventos** e execute as seguintes ações:
   a. Na lista de gravidade do evento, selecione **Aviso**.
   b. Na lista de eventos correspondentes, selecione **Telnet Protocol Enabled**.
6. Clique em **Ações** e selecione o nome do usuário que receberá o e-mail de alerta no campo **Alertar estes usuários**.
7. Configure outras opções nesta página para a frequência de notificação, a emissão de traps SNMP e a execução de um script.
8. Clique em **Salvar**.

Desative eventos de segurança específicos no Active IQ Unified Manager

Todos os eventos estão ativados por padrão. Você pode desativar eventos específicos para impedir a geração de notificações para aqueles que não são importantes no seu ambiente. Você pode ativar eventos desativados se desejar voltar a receber notificações para eles.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Ao desativar eventos, os eventos gerados anteriormente no sistema são marcados como obsoletos e os alertas configurados para esses eventos não são acionados. Ao ativar eventos desativados, 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 eventos**.
2. Na página **Event** Setup, desative ou ative eventos escolhendo uma das seguintes opções:

Se você quiser…	Então faça isso…
Desativar eventos	a. Clique em **Desativar**. b. Na caixa de diálogo Disable Events, selecione a gravidade **Warning**. Esta é a categoria para todos os eventos de segurança. c. Na coluna Eventos correspondentes, selecione os eventos de segurança que deseja desativar e clique na seta para a direita para movê-los para a coluna Desativar eventos. d. Clique em **Salvar e fechar**. e. Verifique se os eventos que você desativou são exibidos na exibição em lista da página Configuração de Eventos.
Ativar eventos	a. Na lista de eventos desativados, selecione a caixa de seleção do evento, ou dos eventos, que você deseja reativar. b. Clique em **Enable**.

Visualize eventos de segurança no Active IQ Unified Manager

Os eventos de segurança fornecem a você informações sobre o status de segurança dos clusters do ONTAP, das máquinas virtuais de storage (SVMs) e dos volumes, com base nos parâmetros definidos no *NetApp Security Hardening Guide for ONTAP 9*. Esses eventos notificam você sobre possíveis problemas para que você possa avaliar a gravidade deles e corrigir o problema, se necessário.

Os eventos de segurança são agrupados por tipo de origem e incluem o nome do evento e do trap, o nível de impacto e a gravidade. Esses eventos aparecem nas categorias de eventos do cluster e da storage VM.

Gerencie operações de backup e restauração

Gerencie as operações de backup e restauração no Active IQ Unified Manager

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 o Unified Manager está instalado e do número de clusters e nós gerenciados:

Sistema operacional	Tamanho da implantação	Método de backup recomendado
O VMware vSphere	Qualquer	Snapshot do VMware do dispositivo virtual do Unified Manager
O Red Hat Enterprise Linux	Pequeno	Dump do banco de dados MySQL do Unified Manager
	Grande	NetApp Snapshot do banco de dados do Unified Manager
O Microsoft Windows	Pequeno	Dump do banco de dados MySQL do Unified Manager
	Grande	NetApp Snapshot do banco de dados do Unified Manager com o protocolo iSCSI

As seções a seguir descrevem esses diferentes métodos.

Backup e restauração do Active IQ Unified Manager em um appliance virtual

O modelo de backup e restauração do Unified Manager, quando instalado em um dispositivo virtual, consiste em capturar e restaurar uma imagem completa da aplicação virtual.

As seguintes tarefas permitem que você conclua um backup do dispositivo virtual:

1. Desligue a máquina virtual e crie um Snapshot do VMware do appliance virtual do Unified Manager.
2. Faça uma cópia Snapshot da NetApp no datastore para capturar o snapshot do VMware.

   Se o datastore não estiver hospedado em um sistema que execute o software ONTAP, siga as diretrizes do fornecedor de storage para criar um backup do Snapshot do VMware.

3. Replique a cópia Snapshot da NetApp, ou o equivalente de snapshot, para um armazenamento alternativo.
4. Exclua o snapshot do VMware.

Você deve implementar um cronograma de backup usando estas tarefas para garantir que o appliance virtual do Unified Manager esteja protegido caso surjam problemas.

Para restaurar a VM, você pode usar o snapshot do VMware que você criou para restaurar a VM ao estado do backup em um ponto no tempo.

Backup e restauração usando um dump de banco de dados MySQL

Backup e restauração usando um dump do banco de dados MySQL no Active IQ Unified Manager

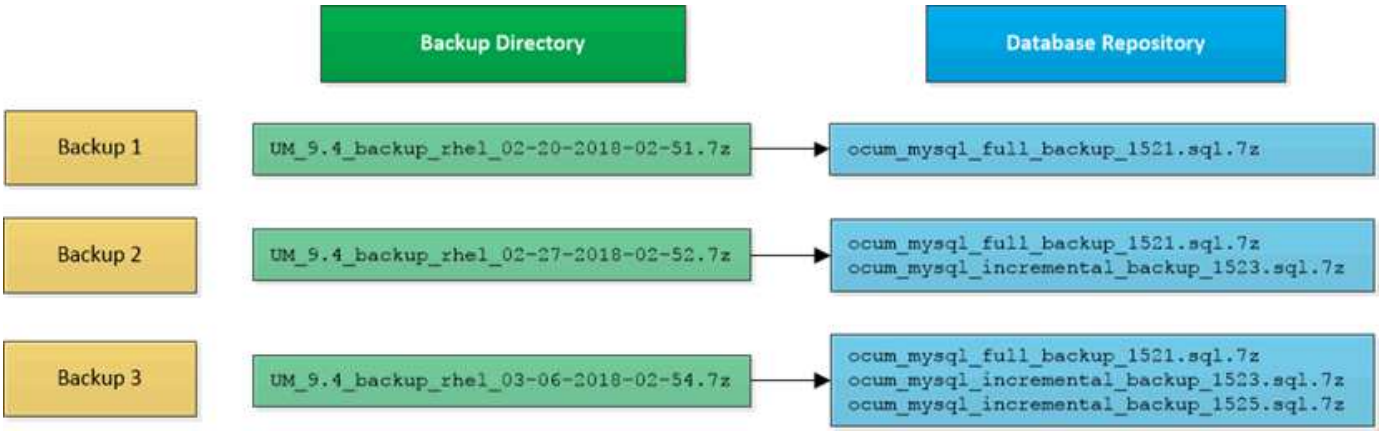
Um backup de dump do banco de dados MySQL é uma cópia do banco de dados e dos arquivos de configuração do Active IQ Unified Manager que você pode usar em caso de falha do sistema ou perda de dados. Você pode agendar um backup para ser gravado

em um destino local ou em um destino 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 ou Windows. No entanto, se o Unified Manager estiver gerenciando um grande número de clusters e nós, ou se seus backups do MySQL estiverem levando muitas horas para serem concluídos, você poderá fazer backup usando cópias Snapshot. Essa funcionalidade está disponível no Red Hat Enterprise Linux e no Windows.

Um backup de dump do banco de dados consiste em um único arquivo no diretório de backup e um ou mais arquivos no diretório do repositório do 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, 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 gera um backup, um único arquivo é criado no diretório de backup e um arquivo de backup incremental é criado no diretório do repositório do banco de dados, contendo as diferenças em relação ao arquivo de backup completo. Esse processo continua à medida que você cria backups adicionais, até a configuração máxima de retenção, conforme mostrado na figura a seguir.



Não renomeie nem remova nenhum dos arquivos de backup nesses dois diretórios, caso contrário qualquer operação de restauração subsequente falhará.

Se você gravar seus arquivos de backup no sistema local, deverá iniciar um processo para copiar esses arquivos de backup para um local remoto, para que estejam disponíveis caso ocorra um problema no sistema que exija uma restauração completa.

Antes de iniciar uma operação de backup, o Active IQ Unified Manager realiza uma verificação de integridade para verificar se todos os arquivos e diretórios de backup necessários existem e podem ser gravados. Ele também verifica se há espaço suficiente no sistema para criar o arquivo de backup.

Configure as definições de backup de dump do banco de dados no Active IQ Unified Manager

Você pode configurar as definições de backup de dump do banco de dados do Unified Manager para definir o caminho de backup do banco de dados, a contagem de retenção e a programação de backups. Você pode ativar backups agendados diários ou semanais. Por padrão, os backups agendados estão desativados, mas você deve definir uma

programação de backups.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Você deve ter no mínimo 150 GB de espaço disponível no local que você definir como o caminho de backup.

  Recomenda-se que você use um local remoto externo ao sistema host do Unified Manager.

- Quando o Unified Manager estiver instalado em um sistema Linux e você estiver 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.

A primeira execução de um backup exige mais tempo do que os 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, 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 Snapshot.
- O backup realizado durante os primeiros 15 dias após a adição de um novo cluster pode não ser preciso o suficiente para obter dados históricos de desempenho.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **backup do 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, o número de retenções e o agendamento.

   O valor padrão para a contagem de retenção é 10; você pode usar 0 para criar backups ilimitados.

4. Selecione o botão **Agendado Diariamente** ou **Agendado Semanalmente** e em seguida especifique os detalhes do agendamento.
5. Clique em **Aplicar**.

Os arquivos de backup do banco de dados são criados com base no agendamento. Você pode ver os arquivos de backup disponíveis na página Backup do Banco de Dados.

Saiba mais sobre restauração de banco de dados no Active IQ Unified Manager

A restauração de um banco de dados MySQL é o processo de restaurar um arquivo de backup existente do Unified Manager para o mesmo servidor do Unified Manager ou para um servidor diferente do Unified Manager. 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, poderá executar a opção de restauração usando o local padrão. Se você estiver executando uma operação de restauração em um sistema Unified Manager diferente (um sistema remoto), deverá copiar o arquivo de backup, ou os arquivos de backup, do storage secundário para o disco local antes de executar a opção de restauração.

Durante o processo de restauração, você sairá 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.

Os arquivos de backup antigos não podem ser usados para restaurar uma imagem após o Unified Manager ser 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"

"Habilitar autenticação SAML"

"Autenticação com Active Directory ou OpenLDAP"

Restaurar um backup de banco de dados MySQL em um sistema Linux no Active IQ Unified Manager

Se ocorrer perda de dados ou corrupção de dados, você poderá restaurar o Unified Manager ao estado estável anterior com perda mínima de dados. Você pode restaurar o banco de dados do Unified Manager em um sistema local ou remoto Red Hat Enterprise Linux usando o console de manutenção do Unified Manager.

Antes de começar

- Você precisa ter as credenciais do usuário raiz para o host Linux no qual o Unified Manager está instalado.
- Você precisa ter um ID de usuário e uma senha autorizados para fazer login no console de manutenção do servidor Unified Manager.
- Você deve ter copiado o arquivo de backup do Unified Manager e o conteúdo do diretório do repositório do banco de dados para o sistema no qual realizará a operação de restauração.

  Recomenda-se que você copie o arquivo de backup para o diretório padrão `/data/ocum`-backup. Os arquivos do repositório do banco de dados devem ser copiados para o subdiretório `/database-dumps-repo` no diretório `/ocum-backup`.

- Os arquivos de backup devem ser do tipo `.7z`.

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. Você pode restaurar um arquivo de backup do Linux ou um arquivo de backup de appliance virtual para um sistema Red Hat Enterprise Linux.

Se o nome da pasta de backup contiver um espaço, você deverá incluir o caminho absoluto ou relativo entre aspas duplas.

Passos

1. Se você estiver realizando uma restauração em um novo servidor, após instalar o Unified Manager, não inicie a UI nem configure clusters, usuários ou configurações de autenticação quando a instalação estiver concluída. O arquivo de backup preenche essas informações durante o processo de restauração.
2. Usando o Secure Shell, conecte-se ao endereço IP ou ao nome de domínio totalmente qualificado do sistema Unified Manager.
3. Faça login no sistema com o nome e a senha do usuário de manutenção (umadmin).
4. Digite o comando `maintenance_console` e pressione Enter.
5. No console de manutenção, no **Main Menu**, insira o número da opção **Backup Restore**.
6. Digite o número para **Restore MySQL Backup**.
7. Quando solicitado, insira o caminho absoluto do arquivo de backup.

   ```
   Bundle to restore from: /data/ocum-
   backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
   ```

   Após a conclusão da operação de restauração, você poderá fazer login no Unified Manager.

Após restaurar o backup, se o servidor do OnCommand Workflow Automation não funcionar, execute as seguintes etapas:

1. No servidor do Workflow Automation, altere o endereço IP do servidor do Unified Manager para apontar para a máquina mais recente.
2. No servidor do Unified Manager, redefina a senha do banco de dados se a aquisição falhar na etapa 1.

Restaurar um backup de banco de dados MySQL no Windows no Active IQ Unified Manager

Em caso de perda de dados 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 precisa 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 realizará a operação de restauração.

  Recomenda-se 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 no diretório `\backup`.

- Os arquivos de backup devem ser do tipo `.7z`.

O recurso de restauração é específico da plataforma e da versão. Você pode restaurar um backup 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 realizando uma restauração em um novo servidor, após instalar o Unified Manager, não inicie a UI nem configure clusters, usuários ou configurações de autenticação quando a instalação estiver concluída. O arquivo de backup preenche essas informações durante o processo de restauração.
2. Faça login no sistema Unified Manager com as 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, no **Main Menu**, insira o número da opção **Backup Restore**.
6. Digite o número para **Restore MySQL Backup**.
7. Quando solicitado, insira o caminho absoluto do arquivo de backup.

```
Bundle to restore from:
\ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac
kup_windows_02-20-2020-02-51.7z
```

   Após a conclusão da operação de restauração, você poderá fazer login no Unified Manager.

Após restaurar o backup, se o servidor do OnCommand Workflow Automation não funcionar, execute as seguintes etapas:

1. No servidor do Workflow Automation, altere o endereço IP do servidor do Unified Manager para apontar para a máquina mais recente.
2. No servidor do Unified Manager, redefina a senha do banco de dados se a aquisição falhar na etapa 1.

Backup e restauração usando NetApp Snapshots

Backup e restauração usando NetApp Snapshots no Active IQ Unified Manager

Uma NetApp cópia Snapshot cria uma imagem pontual do banco de dados e dos arquivos de configuração do Unified Manager que você pode usar para restaurar em caso de falha do sistema ou perda de dados. Você agenda uma cópia Snapshot para ser gravada periodicamente em um volume de um dos seus clusters ONTAP para que sempre tenha uma cópia atual.

Essa funcionalidade não está disponível para o Active IQ Unified Manager instalado em um appliance virtual.

Configure backup no Linux no Active IQ Unified Manager

Se o seu Active IQ Unified Manager estiver instalado em uma máquina Linux, você poderá configurar o backup e a restauração usando NetApp Snapshots.

As cópias Snapshot levam muito pouco tempo, geralmente apenas alguns minutos, e o banco de dados do Unified Manager fica bloqueado por um período muito curto, de modo que há muito pouca interrupção na sua

instalação. A imagem consome um espaço de storage mínimo e gera uma sobrecarga de desempenho insignificante, pois registra apenas as alterações nos arquivos desde que a última cópia Snapshot foi criada. Como o Snapshot é criado em um cluster ONTAP, você pode aproveitar outros recursos da NetApp, como o SnapMirror, para criar proteção secundária, se necessário.

Antes de iniciar uma operação de backup, o Unified Manager realiza uma verificação de integridade para confirmar se o sistema de destino está disponível.

- Você só pode restaurar uma cópia Snapshot na mesma versão do Active IQ Unified Manager.

  Por exemplo, se você criou um backup no Unified Manager 9.18, o backup só pode ser restaurado em sistemas do Unified Manager 9.18.

- Se houver qualquer alteração na configuração de Snapshot, isso poderá invalidá-lo.

Configure o local da cópia Snapshot no Active IQ Unified Manager

Você pode configurar o volume em que as cópias Snapshot serão armazenadas em um dos seus clusters ONTAP usando o ONTAP System Manager ou a ONTAP CLI.

Antes de começar

O cluster, a máquina virtual de armazenamento e o volume devem atender aos seguintes requisitos:

- Requisitos do cluster:
  - Você deve instalar o ONTAP 9.3 ou superior
  - Deve estar geograficamente próximo ao servidor do Unified Manager
  - Você pode monitorá-lo pelo Unified Manager, mas isso não é obrigatório
- Requisitos da VM de storage:
  - A comutação de nomes e o mapeamento de nomes devem ser configurados para usar “files”
  - Usuários locais criados para corresponder aos usuários do lado do cliente
  - Certifique-se de que todo o acesso de leitura/gravação esteja selecionado
  - Certifique-se de que o Superuser Access esteja definido como “any” na política de exportação
  - NFS para NetApp Snapshot para Linux
  - O NFSv4 deve estar habilitado no servidor NFS, e o domínio de ID do NFSv4 deve estar especificado no cliente e na VM de storage
  - O volume deve ter pelo menos o dobro do tamanho do diretório /opt/netapp/data do Unified Manager

    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 desativada
  - O dimensionamento automático de volume deve estar ativado
  - O nível de serviço de desempenho deve ser definido para uma política com alto IOPS e baixa latência, como “Extreme”

Para obter instruções detalhadas sobre como criar o volume NFS, consulte "Como configurar o NFSv4 no ONTAP 9" e o "Guia expresso de configuração de NFS do ONTAP 9".

Especifique o local de destino para as cópias Snapshot no Active IQ Unified Manager

Você deve configurar o local de destino para as cópias Snapshot do Active IQ Unified Manager 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 precisa ter as credenciais do usuário raiz do host Linux no qual o Active IQ Unified Manager está instalado.
- Você precisa ter um ID de usuário e uma senha autorizados para fazer login no console de manutenção do servidor Unified Manager.
- Você deve ter o endereço IP de gerenciamento do cluster, o nome da máquina virtual de storage, o nome do volume e o nome de usuário e a senha do sistema de storage.
- Você deve ter montado o volume no host do Active IQ Unified Manager e deve ter o caminho de montagem.

Passos

1. Utilize o Secure Shell para conectar-se ao endereço IP ou FQDN do sistema Active IQ Unified Manager.
2. Faça login no sistema com o nome e a senha do usuário de manutenção (umadmin).
3. Digite o comando `maintenance_console` e pressione Enter.
4. No console de manutenção, no **Main Menu**, insira o número da opção **Backup Restore**.
5. Digite o número de **Configure NetApp Snapshot Backup**.
6. Digite o número para configurar NFS.
7. Analise as informações que você precisará fornecer e, em seguida, insira o número para **Inserir detalhes da configuração de backup**.
8. Para identificar o volume em que o Snapshot será gravado, insira o endereço IP da interface de gerenciamento do cluster, o nome da VM de storage, o nome do volume, o nome do LUN, o nome de usuário e a senha do sistema de storage 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 Snapshot, caso você ainda não tenha feito isso.

O Active IQ Unified Manager oferece suporte a backup e restauração usando NetApp Snapshots no sistema operacional Windows com a ajuda de LUNs usando o protocolo iSCSI.

O backup baseado em Snapshot pode ser realizado 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, impedindo qualquer gravação simultânea. Para que o seu sistema do Unified Manager instalado no sistema operacional Windows execute backup e restauração usando NetApp Snapshots, você deve primeiro configurar o backup do Unified Manager para ser baseado em Snapshot usando o console de manutenção.

Antes de configurar o Unified Manager para criar cópias Snapshot, você deve executar as seguintes tarefas de configuração.

- Configurar cluster do ONTAP
- Configurar a máquina host do Windows

Configure um local de backup para o Active IQ Unified Manager no Windows

Você deve configurar o volume para armazenar cópias Snapshot após fazer backup do Unified Manager no Windows.

Antes de começar

O cluster, a máquina virtual de armazenamento e o volume devem atender aos seguintes requisitos:

- Requisitos do cluster:
  - Você deve instalar o ONTAP 9.3 ou superior
  - Deve estar geograficamente próximo ao servidor do Unified Manager
  - É monitorado pelo Unified Manager
- Requisitos da VM de storage:
  - Conectividade iSCSI no cluster ONTAP
  - O protocolo iSCSI deve estar habilitado na máquina configurada
  - Você deve ter um volume e um 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 o dobro do tamanho dos dados que se espera processar no Active IQ Unified Manager 9.9.

    Isso também estabelece o mesmo requisito de tamanho para o volume.
  - Certifique-se de que todo o acesso de leitura/gravação esteja selecionado
  - Certifique-se de que o Superuser Access esteja definido como “any” 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 estar definido como Windows
  - A política de Snapshot local deve ser desativada

- O dimensionamento automático de volume deve estar ativado
- O nível de serviço de desempenho deve ser definido para uma política com alto IOPS e baixa latência, como “Extreme”

Configure um cluster ONTAP para backup e restauração no Active IQ Unified Manager

Você precisa executar algumas etapas de pré-configuração nos clusters do ONTAP antes de fazer backup e restaurar o Active IQ Unified Manager usando cópia Snapshot 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 configurar LIFs de dados para que fiquem disponíveis para serem atribuídas como LIFs iSCSI à VM de storage. A próxima etapa é configurar uma VM de storage habilitada para iSCSI usando a interface de usuário do System Manager. Você precisará configurar uma rota de rede estática para esta VM de storage para controlar como as LIFs usam a rede para o tráfego de saída.

Você deve ter um volume dedicado e um LUN para configuração de backup. O volume selecionado deve incluir apenas um LUN. O tamanho do LUN deve ser pelo menos o dobro do tamanho dos dados que devem ser processados pelo Active IQ Unified Manager.

Você precisa realizar a seguinte configuração:

Passos

1. Configure uma VM de storage habilitada para iSCSI ou use uma VM de storage existente que tenha a mesma configuração.
2. Configure uma rota de rede para a VM de storage configurada.
3. Configure um volume com capacidade adequada e um único LUN dentro dele, garantindo que o volume seja dedicado exclusivamente a esse LUN.

   Em um cenário em que o LUN é criado no System Manager, 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 storage.
5. Configure um portset.
6. Integre o igroup com o portset.
7. Mapeie o LUN para o igroup.

Configure uma máquina host Windows no Active IQ Unified Manager

Você precisa configurar sua máquina host Windows antes que possa usar o NetApp Snapshot para fazer backup e restauração do 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 **iSCSI Initiator**.

Antes de começar

Você deve limpar quaisquer configurações anteriores na máquina host.

Se você estiver tentando iniciar o iniciador iSCSI em uma instalação nova do Windows, será solicitada uma confirmação e, após você confirmá-la, 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 que está inativo ou tentando se conectar. Portanto, você precisará garantir que todas as configurações anteriores

no host Windows sejam removidas.

Passos

1. Limpe quaisquer configurações anteriores na máquina host.
2. Descubra o portal de destino.
3. Conecte-se ao portal de destino.
4. Conecte-se usando multipath ao portal de destino.
5. Descubra os dois LIFs.
6. Descubra a LUN configurada 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 Snapshot no Windows no Active IQ Unified Manager

Você deve configurar o local de destino para as cópias Snapshot do Active IQ Unified Manager 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 precisa ter privilégios de administrador no host Windows onde o Active IQ Unified Manager está instalado.
- Você precisa ter um ID de usuário e uma senha autorizados para fazer login no console de manutenção do servidor Unified Manager.
- Você precisa ter o endereço IP de gerenciamento do cluster, o nome da máquina virtual de storage, o nome do volume, o nome da LUN e o nome de usuário e a senha do sistema de storage.
- Você deve ter montado o volume como uma unidade de rede no host do Active IQ Unified Manager e deve ter a unidade montada.

Passos

1. Usando o Power Shell, conecte-se ao endereço IP ou ao domínio totalmente qualificado do sistema Active IQ Unified Manager.
2. Faça login no sistema com o nome e a senha do usuário de manutenção (umadmin).
3. Digite o comando `maintenance_console` e pressione Enter.
4. No console de manutenção, no **Main Menu**, insira o número da opção **Backup Restore**.
5. Digite o número de **Configure NetApp Snapshot Backup**.
6. Digite o número para configurar iSCSI.
7. Analise as informações que você precisará fornecer e, em seguida, insira o número para **Inserir detalhes da configuração de backup**.
8. Para identificar o volume no qual a Snapshot será gravada, insira o endereço IP da interface de gerenciamento do cluster, o nome da VM de storage, o nome do volume, o nome da LUN, o nome de usuário e a senha do sistema de storage e a unidade de montagem.
9. Verifique essas informações e insira `y`.

   O sistema executa as seguintes tarefas:

   - A VM de storage foi validada
   - O volume foi validado

- A unidade montada e o status são validados
- Existência e status da LUN
- Existência da unidade de rede
- A existência de espaço recomendado (mais do que o dobro do diretório de dados do MySQL) no volume montado é validada
- Caminho da LUN correspondente à LUN dedicada 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 Snapshot.

Configure um backup Snapshot a partir do console de manutenção no Active IQ Unified Manager

Para fazer o backup do Active IQ Unified Manager usando cópia Snapshot, você deve executar algumas etapas de configuração no console de manutenção.

Antes de começar

Você deve ter os seguintes detalhes para o seu sistema:

- Endereço IP do cluster
- Nome da VM de 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 **Update NetApp Snapshot Backup Configuration**. Você só pode atualizar a senha.

4. No menu, digite 1 para selecionar **Configurar o NetApp Snapshot Backup**.
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 a LUN está montada no host.

   Em seguida, o processo verifica se o diretório de dados, o caminho do LUN, a VM de armazenamento, os volumes, a disponibilidade de espaço, a unidade e outros dados fornecidos por você estão corretos. As operações que ocorrem em segundo plano são:

   - Os serviços estão interrompidos

- O diretório do banco de dados foi movido para o armazenamento montado
- O diretório do banco de dados é excluído e links simbólicos são criados
- Os serviços são reiniciados após a conclusão da configuração na interface do Active IQ Unified Manager, e o tipo de backup é modificado para NetApp Snapshot e é exibido na interface de usuário como backup de banco de dados (baseado em Snapshot).

Antes de iniciar uma operação de backup, você deve verificar se houve alguma alteração na configuração do Snapshot, pois isso pode fazer com que o Snapshot se torne inválido. Suponha que você configurou o backup na unidade G e criou um Snapshot. Mais tarde, você reconfigurou o backup para a unidade E, e os dados são salvos na unidade E de acordo com a nova configuração. Se você tentar restaurar o Snapshot criado quando ele estava na unidade G, a operação falhará com o erro de que a unidade G não existe.

Defina um cronograma de backup para Linux e Windows no Active IQ Unified Manager

Você pode usar a interface do usuário do Unified Manager para configurar a programação em que as cópias Snapshot do Unified Manager são criadas.

Antes de começar

- Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
- Você deve ter configurado as definições para criar cópias Snapshot no console de manutenção para identificar o destino onde as cópias Snapshot serão criadas.

As cópias Snapshot são criadas em apenas alguns minutos, e o banco de dados do Unified Manager fica bloqueado por apenas alguns segundos.

O backup realizado durante os primeiros 15 dias após a adição de um novo cluster pode não ser preciso o suficiente para obter dados históricos de desempenho.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **backup do banco de dados**.
2. Na página **Backup do Banco de Dados**, clique em **Configurações de Backup**.
3. Insira o número máximo de cópias Snapshot que você deseja manter no campo **Retention Count**.

   O valor padrão da contagem de retenção é 10. O número máximo de cópias Snapshot é determinado pela versão do software ONTAP no cluster. Você pode deixar este campo em branco para implementar o valor máximo independentemente da versão do ONTAP.

4. Selecione o botão **Agendado Diariamente** ou **Agendado Semanalmente** e em seguida especifique os detalhes do agendamento.
5. Clique em **Aplicar**.

As cópias Snapshot são criadas com base no agendamento. Você pode ver os arquivos de backup disponíveis na página Database Backup.

Devido à importância deste volume e dos Snapshots, você pode criar um ou dois alertas para este volume para receber uma notificação quando ocorrer qualquer uma destas situações:

- O espaço do volume está 90% cheio. Use o evento **Espaço do volume cheio** para configurar o alerta.

  Você pode adicionar capacidade ao volume usando o ONTAP System Manager ou a ONTAP CLI para que o banco de dados do Unified Manager não fique sem espaço.

- O número de snapshots está próximo de atingir o número máximo. Use o evento **Too Many Snapshot Copies** para configurar o alerta.

  Você pode excluir snapshots mais antigos usando o ONTAP System Manager ou a ONTAP CLI para que sempre haja espaço para novas cópias Snapshot.

Você configura os alertas na página Configuração de Alertas.

Restaure o Active IQ Unified Manager usando cópias do Snapshot

Se ocorrer perda de dados ou corrupção de dados, você poderá restaurar o Unified Manager ao estado estável anterior com perda mínima de dados. Você pode restaurar o banco de dados Snapshot do Unified Manager em um sistema operacional local ou remoto usando o console de manutenção do Unified Manager.

Antes de começar

- Você deve ter as credenciais do usuário raiz para o host Linux e privilégios administrativos para a máquina host Windows na qual o Unified Manager está instalado.
- Você precisa ter um ID de usuário e uma senha autorizados para fazer login no console de manutenção do servidor 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: Secure Shell
   - Windows: PowerShell
2. Faça login no sistema com as credenciais do usuário raiz.
3. Digite o comando `maintenance_console` e pressione Enter.
4. No console de manutenção, no **Main Menu**, digite 4 para a opção **Backup Restore**.
5. Digite 2 para selecionar **Backup and Restore using NetApp Snapshot**.

   Se você estiver executando uma restauração em um novo servidor, após instalar o Unified Manager, não inicie a interface de usuário nem configure clusters, usuários ou configurações de autenticação quando a instalação estiver concluída. Digite 1 para selecionar **Configure NetApp Snapshot Backup** e configure as definições para cópias Snapshot como estão no sistema original.
6. Digite 3 para selecionar **Restaurar usando NetApp Snapshot**.
7. Selecione a cópia Snapshot a partir da qual deseja restaurar o Unified Manager. Pressione **Enter**.
8. Após a conclusão do processo de restauração, faça login na interface de usuário do Unified Manager.

Após restaurar o backup, se o servidor do Workflow Automation não funcionar, execute as seguintes etapas:

1. No servidor do Workflow Automation, altere o endereço IP do servidor do Unified Manager para apontar para a máquina mais recente.
2. No servidor do Unified Manager, redefina a senha do banco de dados se a aquisição falhar na etapa 1.

Modifique o tipo de backup no Active IQ Unified Manager

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 Snapshot da NetApp** permite que você volte a usar o backup baseado em MySQL.

Antes de começar

Você precisa ter um ID de usuário e uma senha autorizados para fazer login no console de manutenção do servidor Unified Manager.

Passos

1. Acesse o console de manutenção.
2. Selecione 4 no **Main Menu** para backup e restauração.
3. Selecione 2 no **Menu de backup e restauração**.
4. Selecione 4 para **Desconfigurar o backup Snapshot da NetApp**.

   As ações realizadas são exibidas, que são parar os serviços, desfazer o link simbólico, mover os dados do storage para o diretório e, em seguida, iniciar os serviços novamente.

   Depois que o método de backup é modificado, o mecanismo de backup é alterado de cópia Snapshot para o backup padrão do MySQL. Essa alteração aparece na seção Backup do Banco de Dados das configurações gerais.

Entenda o backup sob demanda para o Active IQ 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 em Snapshot da NetApp.

Você pode realizar backup sob demanda usando o botão **Backup Now** 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 o Active IQ Unified Manager appliance virtual para um sistema Linux

Você pode restaurar um backup de dump do banco de dados MySQL do Unified Manager de um appliance virtual para um sistema Red Hat Enterprise Linux se desejar alterar o sistema operacional host no qual o Unified Manager está em execução.

Antes de começar

- No dispositivo virtual:
  - Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.
  - Você precisa 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 clusters, usuários ou definições 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 do usuário raiz para o host Linux.

Estas etapas descrevem como criar um arquivo de backup no dispositivo virtual, copiar os arquivos de backup para o Red Hat Enterprise Linux e, em seguida, restaurar o backup do banco de dados no 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 de backup para /jail/support.
4. Na seção Agendamento, selecione **Agendado diariamente** e insira um horário alguns minutos após o horário atual para que o backup seja criado em seguida.
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 terminar.

7. Faça login como usuário raiz no host Linux onde o Unified Manager está instalado e copie os arquivos de backup de /support no appliance virtual usando SCP.`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

   ```
   root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
   ```

   Certifique-se de ter copiado o arquivo de backup .7z e todos os arquivos de repositório .7z no subdiretório /database-dumps-repo.

8. No prompt de comando, restaure o backup: `um backup restore -f /<backup_file_path>/<backup_file_name>`

   ```
   um backup restore -f /UM_9.7.N151113.1348_backup_unix_02-12-2019-04-16.7z
   ```

9. Após a conclusão da operação de restauração, faça login na interface da Web do Unified Manager.

Você deve realizar 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, pois não existe um caminho /jail/support no sistema Linux.
- Reconfigure ambos os lados da sua conexão com o Workflow Automation, caso você esteja usando o WFA.
- Reconfigure as configurações de autenticação SAML, se você estiver usando SAML.

Após 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

Gerencie scripts no Active IQ Unified Manager

Você pode usar scripts para modificar ou atualizar automaticamente vários objetos de armazenamento no Unified Manager. O script está associado a um alerta. Quando um evento aciona um alerta, o script é executado. Você pode carregar scripts personalizados e testar sua execução quando um alerta é gerado.

A capacidade de carregar scripts no Unified Manager e executá-los está habilitada por padrão. Se sua organização não quiser permitir essa funcionalidade por motivos de segurança, você pode desativá-la em **Storage Management** > **Feature Settings**.

Entenda como os scripts funcionam com alertas no Active IQ Unified Manager

Você pode associar um alerta ao seu script para que ele seja executado quando um alerta for acionado para um evento no Unified Manager. Você pode usar os scripts para resolver problemas com objetos de armazenamento ou identificar quais objetos de armazenamento estão gerando os eventos.

Quando um alerta é gerado para um evento no Unified Manager, um e-mail de alerta é enviado aos destinatários especificados. Se você associou um alerta a um script, o script é executado. Você pode obter os detalhes dos argumentos passados para o 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 "Fix it" não estarão disponíveis por padrão na página Management Actions nem no dashboard do Unified Manager.

O script utiliza os seguintes argumentos para execução:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Você pode usar os argumentos em seus scripts e coletar informações sobre eventos relacionados ou modificar objetos de armazenamento.

Exemplo de obtenção de argumentos a partir 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 no Active IQ Unified Manager

Você pode adicionar scripts no Unified Manager e associar os scripts a alertas. Esses scripts são executados automaticamente quando um alerta é gerado e permitem que você obtenha informações sobre os 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 compatíveis 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 em Perl, Python e Shell
Windows	PowerShell, scripts Perl, Python e .bat

  - Para scripts em Perl, o Perl deve estar instalado no servidor do Unified Manager. Para instalações do VMware, o Perl 5 é instalado por padrão, e os scripts oferecerão suporte apenas ao que o Perl 5 suporta. Se o Perl foi instalado após o Unified Manager, você deve reiniciar o servidor do Unified Manager.
  - Para scripts PowerShell, a política de execução apropriada do PowerShell deve ser configurada no servidor Windows para que os scripts possam ser executados.

> Se o seu script criar arquivos de log para acompanhar o progresso do script de alerta, você deve garantir que esses arquivos de log não sejam criados em nenhum lugar dentro da pasta de instalação do Unified Manager.

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Você pode fazer upload de scripts personalizados e coletar detalhes do evento sobre o alerta.

> Se você não visualizar essa funcionalidade na interface de usuário, é porque seu administrador a desativou. Se necessário, você pode ativá-la 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 **Add**.

Excluir scripts no Active IQ Unified Manager

Você pode excluir um script do Unified Manager quando ele não for mais necessário ou válido.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- O script não deve estar associado a um alerta.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Scripts**.
2. Na página **Scripts**, selecione o script que deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

Execução de script de teste no Active IQ Unified Manager

Você pode verificar se seu script é executado corretamente quando um alerta é gerado para um objeto de armazenamento.

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você deve ter carregado no Unified Manager um script em um formato de arquivo compatível.

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 à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
4. Na página **Configuração de alertas**, execute uma das seguintes ações:

Para…	Faça isso…
Adicionar um alerta	a. Clique em **Add**. 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 **Alert Setup**, selecione o alerta que você adicionou ou modificou e clique em **Test**.

   O script é executado com o argumento “-test”, e um alerta de notificação é enviado para os endereços de e-mail especificados no momento da criação do alerta.

Gerenciar e monitorar grupos

Entenda grupos

Saiba mais sobre grupos no Active IQ Unified Manager

Um grupo é uma coleção dinâmica de objetos de storage heterogêneo (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 que são monitorados pelo Unified Manager em um determinado momento.

- Cada grupo tem um nome único.
- Você deve configurar pelo menos 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.
- Os 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 simultaneamente ações a todos os objetos de storage em um grupo, como definir limites para volumes.

Entenda como as regras de grupo funcionam para grupos no Active IQ Unified Manager

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 uma regra 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; apenas um tipo de objeto pode ser associado a uma regra de grupo.
- Os 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 para especificar quais objetos de storage estão incluídos no grupo.

As condições dentro de um grupo de condições são executadas usando o operador lógico AND. Todas as condições em um grupo de condições devem ser atendidas. Ao criar ou modificar uma regra de grupo, uma condição é criada para aplicar, selecionar e agrupar apenas os objetos de storage que satisfazem todas as condições do grupo de condições. Você pode usar várias condições dentro de um grupo de condições quando

quiser restringir o escopo de quais objetos de storage incluir em um grupo.

Você pode criar condições com objetos de storage usando os seguintes operandos e operador e especificando o valor necessário.

Tipo de objeto de armazenamento	Operandos aplicáveis
Volume	• Nome do objeto • Nome do cluster proprietário • Nome da SVM proprietária • Anotações
SVM	• Nome do objeto • Nome do cluster proprietário • Anotações
Cluster	• Nome do objeto • Anotações

Ao selecionar a anotação como operando para qualquer objeto de armazenamento, o operador “Is” estará disponível. Para todos os outros operandos, você pode selecionar “Is” ou “Contains” como operador.

- Operando

  A lista de operandos no Unified Manager muda de acordo com o tipo de objeto selecionado. A lista inclui o nome do objeto, o nome do cluster proprietário, o nome da SVM proprietária 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”.

  Ao selecionar o operador “Is”, a condição é avaliada para verificar se o valor do operando corresponde exatamente ao valor fornecido para o operando selecionado.

  Ao selecionar o operador “Contains”, a condição é avaliada para atender a um dos seguintes critérios:

  ◦ O valor do operando corresponde exatamente 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 seguintes duas condições:

- O nome contém “vol”
- O nome da 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

Os grupos de condições são executados usando o operador lógico OU e, em seguida, aplicados aos 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 ampliar o escopo dos objetos de armazenamento a serem incluídos em um grupo.

Exemplo de uma regra de grupo com grupos de condição

Considere dois grupos de condições para um volume, com cada grupo contendo as seguintes duas condições:

- Grupo de condição 1
  - O nome contém “vol”
  - O nome da 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 da anotação data-priority é “critical” O grupo de condições 2 seleciona todos os volumes que incluem “vol” nos nomes e que têm o valor de anotação data-priority como “critical”.

Quando você aplica uma regra de grupo que contém estes dois grupos de condições a objetos de armazenamento, os seguintes objetos de armazenamento são adicionados ao 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”.

Entenda como as ações de grupo funcionam em objetos de armazenamento no Active IQ Unified Manager

Uma ação de grupo é uma operação realizada em todos os objetos de armazenamento de um grupo. Por exemplo, você pode configurar uma ação de grupo de limite de volume para alterar simultaneamente os valores de limite de volume de todos os volumes do grupo.

Os grupos suportam tipos exclusivos de ação de grupo. Você pode ter um grupo com apenas um tipo de ação de grupo de limite de integridade do 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 informa qual ação de grupo se aplica ao objeto de armazenamento.

Exemplo de ações de grupo únicas

Considere um volume A que pertence aos grupos G1 e G2, e as seguintes ações de limite de integridade do volume estão configuradas para esses grupos:

- `Change_capacity_threshold` ação de grupo com classificação 1, para configurar a capacidade do

volume

- `Change_snapshot_copies` ação de grupo com classificação 2, para configurar as cópias Snapshot do volume

A `Change_capacity_threshold` ação de grupo sempre tem prioridade sobre a `Change_snapshot_copies` ação de grupo e é aplicada ao volume A. Quando o Unified Manager conclui um ciclo de monitoramento, os eventos relacionados ao limite de integridade do volume A são reavaliados de acordo com a `Change_capacity_threshold` ação de grupo. Não é possível configurar outro tipo de limite de volume para a ação de grupo, seja para o grupo G1 ou para o grupo G2.

Adicionar grupos no Active IQ Unified Manager

Você pode criar grupos para combinar clusters, volumes e máquinas virtuais de armazenamento (SVMs) para facilitar o gerenciamento.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Você pode definir regras de grupo para adicionar ou remover membros do grupo e para modificar as ações de grupo 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 **Add**.

Editar grupos no Active IQ Unified Manager

Você pode editar o nome e a descrição de um grupo que você criou no Unified Manager.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

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 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 no Active IQ Unified Manager

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 qualquer

regra de grupo associada ao grupo que você deseja excluir.

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Grupos**.
2. Na aba **Grupos**, selecione o grupo que 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 ao grupo. No entanto, essas ações de grupo serão desvinculadas após a exclusão do grupo.

Adicionar regras de grupo no Active IQ Unified Manager

Você pode criar regras de grupo para um grupo para 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 precisa ter a função de Application Administrator ou Storage Administrator.

Os objetos de armazenamento que estão sendo monitorados 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 os seguintes passos 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 da lista disponível.

Para criar….	Faça isso…
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 da lista disponível. e. Clique em **Adicionar condição** para criar mais condições, se necessário, e repita as etapas de a até d para cada condição.

7. Clique em **Add**.

Exemplo de criação de uma regra de grupo

Na caixa de diálogo Adicionar Regra de Grupo, siga estas etapas 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 **Object Name** como operando.
9. Selecione **Contém** como operador.
10. Insira o valor como `vol`.
11. Clique em **Adicionar condição**.
12. Repita os passos de 8 a 10 selecionando **data-priority** como operando no passo 8, **Is** como operador no passo 9 e **critical** como valor no passo 10.
13. Clique em **Adicionar** para criar a condição da regra de grupo.

Editar regras de grupo no Active IQ Unified Manager

Você pode editar as 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 um grupo específico.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Grupos**.

2. Na guia **Regras de Grupo**, selecione a regra de grupo que deseja editar e clique em **Editar**.
3. Na caixa de diálogo **Edit Group Rule**, altere o nome da regra de grupo, o nome do grupo associado, os grupos de condição e as condições conforme necessário.

   Não é possível alterar o tipo de objeto de destino para uma regra de grupo.

4. Clique em **Salvar**.

Excluir regras de grupo no Active IQ Unified Manager

Você pode excluir uma regra de grupo do Active IQ Unified Manager quando ela não for mais necessária.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Quando uma regra de grupo é excluída, os objetos de armazenamento associados serão removidos do grupo.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Grupos**.
2. Na guia **Regras de Grupo**, selecione a regra de grupo que deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

Adicionar ações de grupo no Active IQ Unified Manager

Você pode configurar ações de grupo que deseja aplicar aos objetos de armazenamento em um grupo. Configurar ações para um grupo permite economizar tempo, pois você não precisa adicionar essas ações a cada objeto individualmente.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Grupos**.
2. Na guia **Ações do 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 o grupo para o qual 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 os valores apropriados para os parâmetros necessários para configurar uma ação de grupo.
7. Clique em **Add**.

Editar ações de grupo no Active IQ Unified Manager

Você pode editar os parâmetros da ação de grupo que configurou no Unified Manager,

como o nome da ação de grupo, a descrição, o nome do grupo associado e os parâmetros do tipo de ação.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Grupos**.
2. Na guia **Ações do Grupo**, selecione a ação do grupo que deseja editar e clique em **Editar**.
3. Na caixa de diálogo **Edit Group Action**, altere o nome da ação de grupo, a descrição, o nome do grupo associado e os parâmetros do tipo de ação, conforme necessário.
4. Clique em **Salvar**.

Configure os limites de integridade de volume para grupos no Active IQ Unified Manager

Você pode configurar limites de integridade de volume no nível do grupo para capacidade, cópias Snapshot, cotas de qtree, crescimento e inodes.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

O tipo de ação de grupo "limiar de integridade do volume" se aplica apenas aos volumes de um grupo.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Grupos**.
2. Na guia **Ações do Grupo**, clique em **Adicionar**.
3. Insira um nome e uma descrição para a ação de grupo.
4. Na caixa suspensa **Grupo**, selecione um grupo para o qual você deseja configurar uma ação de grupo.
5. Selecione **tipo de ação** como o 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 integridade.
8. Clique em **Add**.

Excluir ações de grupo no Active IQ Unified Manager

Você pode excluir uma ação de grupo do Unified Manager quando ela não for mais necessária.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Ao excluir a ação de grupo para o limite de integridade do volume, os limites globais são aplicados aos objetos de armazenamento desse grupo. Quaisquer limites de integridade em nível de objeto definidos no objeto de armazenamento não serão afetados.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Grupos**.

2. Na guia **Ações de grupo**, selecione a ação de grupo que deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, confirme a exclusão clicando em **Sim**.

Reordene as ações do grupo no Active IQ Unified Manager

Você pode alterar a ordem das ações de grupo que serão aplicadas aos objetos de armazenamento em um grupo. As ações de grupo são aplicadas aos 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 de acordo com seus requisitos.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Você pode selecionar uma única linha ou várias linhas e, em seguida, executar várias operações de arrastar e soltar para alterar a classificação das ações de grupo. No entanto, você precisa salvar as alterações para que a repriorização seja refletida na grade de ações de grupo.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Grupos**.
2. Na guia **Ações do Grupo**, clique em **Reordenar**.
3. Na caixa de diálogo **Reorder Group Actions**, arraste e solte as linhas para reorganizar a sequência de ações do grupo conforme necessário.
4. Clique em **Salvar**.

Priorize eventos de objetos de storage usando anotações

Entenda melhor as anotações

Saiba mais sobre anotações no Active IQ Unified Manager

Uma anotação é uma cadeia de texto (o nome) atribuída a outra cadeia de texto (o valor). Cada par nome-valor de anotação pode ser associado dinamicamente a objetos de storage usando regras de anotação. Ao associar objetos de storage a anotações predefinidas, você pode filtrar e visualizar os eventos relacionados a eles. Você pode aplicar anotações a clusters, volumes e máquinas virtuais de storage (SVMs).

Cada nome de anotação pode ter vários valores; cada par nome-valor pode ser associado a um objeto de storage por meio de regras.

Por exemplo, você pode criar uma anotação chamada “data-center” com os valores “Boston” e “Canada”. Em seguida, você pode 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”, permitindo que você priorize e resolva o problema.

Entenda como funcionam as regras de anotação no Active IQ 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; apenas um tipo de objeto pode ser associado a uma regra de anotação.
- O Unified Manager adiciona ou remove anotações de objetos de armazenamento após cada ciclo de monitoramento ou quando uma regra é criada, editada, excluída ou reordenada.
- Uma regra de anotação pode ter um ou mais grupos de condições, e cada grupo de condições pode ter uma ou mais condições.
- Os 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 de uma anotação para anotar objetos de armazenamento.

As condições dentro de um grupo de condições são executadas usando o operador lógico AND. Todas as condições em um grupo de condições devem ser atendidas. Ao criar ou modificar uma regra de anotação, uma condição é criada para aplicar, selecionar e anotar apenas os objetos de armazenamento que atendem a todas as condições do grupo de condições. Você pode usar várias condições dentro de um grupo de condições quando quiser restringir o escopo dos objetos de armazenamento a serem anotados.

Você pode criar condições com objetos de storage usando os seguintes operandos e operador e especificando o valor necessário.

Tipo de objeto de armazenamento	Operandos aplicáveis
Volume	• Nome do objeto • Nome do cluster proprietário • Nome da SVM proprietária • Anotações
SVM	• Nome do objeto • Nome do cluster proprietário • Anotações
Cluster	• Nome do objeto • Anotações

Ao selecionar annotation como operando para qualquer objeto de storage, o operador “Is” fica disponível. Para todos os outros operandos, você pode selecionar “Is” ou “Contains” como operador. Ao selecionar o operador “Is”, a condição é avaliada para verificar uma correspondência exata do valor do operando com o valor fornecido para o operando selecionado. Ao selecionar o operador “Contains”, a condição é avaliada para atender a um dos seguintes critérios:

- O valor do operando corresponde exatamente 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 seguintes duas condições:

- O nome contém “vol”
- O nome da SVM é “data_svm”

Esta regra de anotação anota todos os volumes que incluem “vol” em seus nomes e que estão hospedados em SVMs com o nome “data_svm” com a anotação e o tipo de anotação selecionados.

Grupos de condições

Os grupos de condições são executados usando o operador lógico OU e, em seguida, aplicados aos objetos de armazenamento. Os objetos de armazenamento devem atender aos requisitos de um dos grupos de condições para 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 ampliar o escopo dos objetos de armazenamento a serem anotados.

Exemplo de uma regra de anotação com grupos de condições

Considere uma regra de anotação com dois grupos de condições para um volume; cada grupo contém as seguintes duas condições:

- Grupo de condição 1
  - O nome contém “vol”
  - O nome da 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 da anotação 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 da anotação data-priority como “critical”.

Quando uma regra de anotação contendo esses dois grupos de condições é aplicada a 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 têm o valor de anotação de prioridade de dados como “critical”.

Compreenda os valores de anotação predefinidos no Active IQ Unified Manager

Data-priority é uma anotação predefinida que tem os valores Mission critical, High e Low. Esses valores permitem que você anote objetos de storage com base na prioridade dos dados que eles contêm. Você não pode editar nem excluir os valores de anotação predefinidos.

- **Prioridade dos dados:missão crítica**

  Essa anotação é aplicada a objetos de armazenamento que contêm dados essenciais. Por exemplo,

objetos que contêm aplicativos de produção podem ser considerados essenciais.

- **Prioridade dos dados:alta**

  Essa 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 dos dados:baixa**

  Essa anotação é aplicada a objetos de armazenamento que contêm dados de baixa prioridade. Por exemplo, objetos que estão em storage secundário, como destinos de backup e espelhamento, podem ter baixa prioridade.

Adicione anotações dinamicamente no Active IQ Unified Manager

Ao criar anotações personalizadas, o Unified Manager associa dinamicamente clusters, máquinas virtuais de armazenamento (SVMs) e volumes às anotações por meio de regras. Essas regras atribuem automaticamente as anotações aos objetos de armazenamento.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

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 **Add Annotation**, digite um nome e uma descrição para a anotação.
4. Opcional: na seção **Valores da Anotação**, clique em **Adicionar** para adicionar valores à anotação.
5. Clique em **Salvar**.

Adicione valores às anotações no Active IQ Unified Manager

Você pode adicionar valores às anotações e, em seguida, associar objetos de armazenamento a um par nome-valor específico da anotação. Adicionar valores às anotações ajuda a gerenciar objetos de armazenamento com mais eficiência.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Não é possível adicionar valores a anotações predefinidas.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Anotações**.
2. Na página **Anotações**, selecione a anotação à qual deseja adicionar um valor e clique em **Adicionar** na seção **Valores**.
3. Na caixa de diálogo **Adicionar valor de anotação**, especifique um valor para a anotação.

   O valor que você especificar deve ser único para a anotação selecionada.

4. Clique em **Add**.

Excluir anotações no Active IQ Unified Manager

Você pode excluir anotações personalizadas e seus valores quando não forem mais necessários.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- 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 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 no Active IQ Unified Manager

Você pode visualizar a lista de anotações que são associadas dinamicamente a clusters, volumes e máquinas virtuais de storage (SVMs). Você também pode visualizar detalhes como a descrição, criado por, a data de criação, os valores, as 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 de anotações no Active IQ Unified Manager

Você pode excluir valores associados a anotações personalizadas quando esse valor não se aplicar mais à anotação.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- O valor da anotação não deve estar associado a nenhuma regra de anotação ou regra de grupo.

Não é possível excluir valores de anotações predefinidas.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Anotações**.
2. Na lista de anotações na guia **Anotações**, selecione a anotação da qual 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 deixa de ser exibido na lista de valores da anotação selecionada.

Crie regras de anotação no Active IQ Unified Manager

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 precisa ter a função de Application Administrator ou Storage Administrator.

Os objetos de armazenamento que estão sendo monitorados 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 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 da 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 da lista disponível. e. Clique em **Adicionar condição** para criar mais condições, se necessário, e repita as etapas de a até d para cada condição.

7. Clique em **Add**.

Exemplo de criação de uma regra de anotação

Na caixa de diálogo Adicionar Regra de Anotação, siga estes passos 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 da 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 **Object Name** como operando.
9. Selecione **Contém** como operador.
10. Insira o valor como `vol`.
11. Clique em **Adicionar condição**.
12. Repita os passos 8 a 10, selecionando **data-priority** como operando no passo 8, **Is** como operador no passo 9 e **mission-critical** como valor no passo 10.
13. Clique em **Add**.

Adicione anotações manualmente a objetos de storage individuais no Active IQ Unified Manager

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 nome e valor necessária para a anotação.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. Navegue até os objetos de armazenamento que você deseja anotar:

Para adicionar anotação a…	Faça isso…
Clusters	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 **Storage** > **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 no Active IQ Unified Manager

Você pode editar as regras de anotação para modificar os grupos de condições e as condições dentro do grupo de condições para adicionar ou remover anotações dos

objetos de armazenamento.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

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 você 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**.

Configure as condições para as regras de anotação no Active IQ Unified Manager

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 atendem à regra de anotação são anotados com o valor especificado na regra.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

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 e um valor de anotação 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, em que o nome do objeto contém “svm_data”.

Execute as seguintes etapas na caixa de diálogo Add Annotation Rule 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 o operando.
5. Selecione **Contém** como operador.
6. Insira o valor como `svm_data`.
7. Clique em **Add**.

Excluir regras de anotação no Active IQ Unified Manager

Você pode excluir regras de anotação do Active IQ Unified Manager quando elas não forem mais necessárias.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Ao excluir uma regra de anotação, a anotação é desvinculada e removida dos objetos de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Anotações**.
2. Na guia **Regras de Anotação**, selecione a regra de anotação que deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo **Aviso**, clique em **Sim** para confirmar a exclusão.

Reordenar regras de anotação no Active IQ Unified Manager

Você pode alterar a ordem em que o Unified Manager aplica as regras de anotação aos objetos de armazenamento. As regras de anotação são aplicadas aos objetos de armazenamento sequencialmente com base na sua classificação. Ao configurar uma regra de anotação, a classificação é a mais baixa. No entanto, você pode alterar a classificação da regra de anotação de acordo com suas necessidades.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Você pode selecionar uma única linha ou várias linhas e realizar 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 Annotation Rules.

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 precisa salvar as alterações para que a reordenação apareça.

Envie um pacote de suporte pela interface web e pelo console de manutenção

Envie um pacote de suporte através da interface web e do console de manutenção no Active IQ Unified Manager

Você deve enviar um pacote de suporte quando o problema que você está enfrentando exigir um diagnóstico e uma solução de problemas mais detalhados do que uma mensagem AutoSupport pode fornecer. Você pode enviar um pacote de suporte para o suporte técnico usando a interface web do Unified Manager e o console de manutenção.

O Unified Manager armazena, no máximo, dois pacotes de suporte completos e três pacotes de suporte simplificados simultaneamente.

Informações relacionadas

"Funções e capacidades de usuário do Unified Manager"

Envie AutoSupport mensagens para o suporte técnico no Active IQ Unified Manager

A página do AutoSupport permite que você envie mensagens predefinidas e sob demanda do AutoSupport 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, conforme 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 a função de administrador de storage pode gerar e enviar mensagens AutoSupport sob demanda e pacotes de suporte para o suporte técnico. No entanto, somente um administrador ou usuário de manutenção pode habilitar ou desabilitar o AutoSupport periódico e configurar as definições de HTTP, conforme descrito na seção Configurar o servidor proxy HTTP. Em um ambiente que precisa usar um servidor proxy HTTP, a configuração deve estar concluída antes que um administrador de storage possa enviar mensagens AutoSupport sob demanda e pacotes de suporte para o suporte técnico.

Enviar mensagens do 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 deseja enviar a mensagem AutoSupport para o suporte técnico, selecione a caixa de seleção **Enviar para o suporte técnico**.
3. Se você deseja enviar a mensagem do AutoSupport para um destinatário de e-mail específico, selecione 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**.

Ativar periodicamente AutoSupport

Você pode enviar mensagens específicas e predefinidas para o suporte técnico para diagnóstico e resolução de problemas periodicamente. Essa funcionalidade está habilitada por padrão. Caso esteja desabilitada, um administrador ou usuário de manutenção pode ativar as configurações.

Passos

1. Navegue até **Geral** > **AutoSupport**.
2. Na seção Periódico do AutoSupport, selecione a caixa de seleção **Ativar o 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**.

Faça upload do pacote de suporte sob demanda

Você pode gerar e enviar um pacote de suporte ao suporte técnico com base na necessidade de solucionar problemas. O Unified Manager armazena apenas os dois pacotes de suporte gerados mais recentemente. Os pacotes de suporte mais antigos são excluídos do sistema.

Como alguns tipos de dados de suporte podem consumir muitos 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 simplificado que contém apenas 30 dias de logs e registros do banco de dados de configuração; ele exclui dados de desempenho, arquivos de gravação de aquisição e o dump 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 simplificado ao suporte técnico, na janela pop-up Generate and Send Support Bundle, marque a caixa de seleção **Generate light support bundle**.
4. Alternativamente, para enviar um pacote de suporte completo, selecione a caixa de seleção **Gerar pacote de suporte completo**. Selecione os tipos de dados específicos que você deseja incluir ou excluir no pacote de suporte.

   Mesmo que você não selecione nenhum tipo de dados, o pacote de suporte ainda será gerado com outros dados do Unified Manager.

5. Selecione a caixa de seleção **Enviar o pacote para o suporte técnico** para gerar e enviar o pacote para o suporte técnico. Se você não selecionar esta caixa de seleção, o pacote será gerado e armazenado localmente no servidor Unified Manager. O pacote de suporte gerado estará disponível para uso posterior no diretório /support em sistemas VMware, em `/opt/netapp/data/support/` sistemas Linux e em `ProgramData\NetApp\OnCommandAppData\ocum\support` sistemas Windows.
6. Clique em **Enviar**.

Configurar servidor proxy HTTP

Você pode designar um proxy para fornecer acesso à internet a fim de enviar conteúdo do AutoSupport ao suporte técnico se o seu ambiente não fornecer acesso direto pelo servidor do Unified Manager. Esta seção está disponível apenas para administradores e usuários de manutenção.

- **Usar proxy HTTP**

  Marque esta caixa para identificar o servidor usado como proxy HTTP.

  Insira o nome do host ou endereço IP do servidor proxy e o número da porta usada para conectar-se ao servidor.

- **Usar autenticação**

  Marque esta caixa se você precisar fornecer informações de autenticação para acessar o servidor que está sendo usado como proxy HTTP.

  Insira o nome de usuário e a senha necessários para autenticar com o proxy HTTP.

Proxies HTTP que oferecem apenas autenticação básica não são suportados.

Acesse o console de manutenção no Active IQ Unified Manager

Caso a interface de usuário do Unified Manager não esteja em funcionamento, ou se você precisar executar funções que não estão disponíveis na interface de usuário, você pode acessar o console de manutenção para gerenciar seu sistema Unified Manager.

Antes de começar

Você precisa ter instalado e configurado o Unified Manager.

Após 15 minutos de inatividade, o console de manutenção encerra sua sessão.

Quando instalado no VMware, se você já tiver feito login como usuário de manutenção por meio do console do VMware, não poderá fazer login simultaneamente usando o Secure Shell.

Etapa

1. Siga estes passos 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. Faça 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. Faça login no sistema com o nome e a senha do usuário de manutenção (umadmin). c. Digite o comando `maintenance_console` e pressione Enter.

Neste sistema operacional…	Siga estes passos…
Windows	a. Faça login no sistema Unified Manager com as credenciais de administrador. b. Inicie o PowerShell como administrador do Windows. c. Digite o comando `maintenance_console` e pressione Enter.

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

Gere e carregue um pacote de suporte do Active IQ Unified Manager

Você pode gerar um pacote de suporte, contendo informações de diagnóstico, para enviá-lo ao suporte técnico para obter ajuda na resolução 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 a NetApp pelo console de manutenção.

Antes de começar

Você precisa ter acesso ao console de manutenção como o usuário de manutenção.

Como alguns tipos de dados de suporte podem consumir muitos recursos do cluster ou demorar bastante 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. Você também tem a opção de criar um pacote de suporte leve que contenha apenas 30 dias de logs e registros do banco de dados de configuração; ele exclui dados de desempenho, arquivos de gravação de aquisição e o dump de heap do servidor.

O Unified Manager armazena apenas os dois pacotes de suporte gerados mais recentemente. Os pacotes de suporte mais antigos são excluídos do sistema.

Passos

1. No console de manutenção **Main Menu**, selecione **Support/Diagnostics**.
2. Selecione **Generate Light Support Bundle** ou **Generate Support Bundle**, dependendo do nível de detalhes que você deseja ter no pacote de suporte.
3. Se você escolher o pacote de suporte completo, selecione ou desmarque os seguintes tipos de dados para incluir ou excluir do pacote de suporte:

   - **dump do banco de dados**

     Um dump do banco de dados do servidor MySQL.

   - **dump de heap**

     Uma captura instantânea do estado dos principais processos do servidor principal do Unified Manager. Esta opção está desativada por padrão e deve ser selecionada somente quando solicitada pelo suporte ao cliente.

   - **gravações de aquisição**

     Um registro de todas as comunicações entre o Unified Manager e os clusters monitorados.

Mesmo se você desmarcar todos os tipos de dados, o pacote de suporte ainda será gerado com outros dados do Unified Manager.

4. Digite `g`, e pressione Enter para gerar o pacote de suporte.

   Como a geração de um pacote de suporte é uma operação que consome muita memória, você será solicitado a confirmar se realmente deseja gerar o pacote de suporte neste momento.

5. Digite `y`, e pressione Enter para gerar o pacote de suporte.

   Se não desejar gerar o pacote de suporte neste momento, digite `n`, e pressione Enter.

6. Se você incluiu arquivos de despejo do banco de dados no pacote de suporte completo, será solicitado que especifique o período para o qual deseja incluir as estatísticas de desempenho. Incluir estatísticas de desempenho pode consumir muito tempo e espaço, portanto você também pode fazer o despejo do 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. Insira `n` se não desejar que as estatísticas de desempenho sejam incluídas.

   b. Insira o número de dias de estatísticas para incluir, começando às 00h00 da data inicial 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 essas estatísticas serão coletadas.

7. Após a criação do pacote de suporte, você será questionado se deseja enviá-lo para NetApp. Digite `y`, e pressione Enter.

   Você deve inserir o número do seu caso de suporte.

8. Se você já tiver um número de protocolo, digite-o e pressione Enter. Caso contrário, basta pressionar Enter.

   O pacote de suporte foi carregado para a NetApp.

Se o servidor do Unified Manager não estiver conectado à internet ou se você não conseguir fazer upload do 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 de CLI do UNIX ou Linux. Nas 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 capacidades de usuário do Unified Manager"

Recupere o pacote de suporte usando um cliente no Active IQ Unified Manager

Se você for usuário do Windows, pode baixar e instalar uma ferramenta para recuperar o

pacote de suporte do seu servidor do Unified Manager. Você pode enviar o pacote de suporte para o suporte técnico para um diagnóstico mais detalhado do 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 obter 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 você deseja copiar e use a ferramenta para copiar o arquivo do servidor Unified Manager para o seu sistema local.

Recupere o pacote de suporte usando um cliente UNIX ou Linux no Active IQ Unified Manager

Se você for um usuário de UNIX ou Linux, poderá obter 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 obter 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 por Telnet ou pelo console, usando seu servidor cliente Linux.
2. Acesse o diretório /`support`.
3. Recupere o pacote de suporte e copie-o para o diretório local usando o seguinte comando:

Se você estiver usando…	Em seguida, use o seguinte comando…
SCP	`scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`
SFTP	`sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`

   Você recebe o nome do pacote de suporte ao gerá-lo 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 utiliza 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 a partir do Active IQ Unified Manager

Quando um problema exigir informações mais detalhadas de diagnóstico e solução de problemas do que uma mensagem AutoSupport fornece, você pode enviar um pacote de suporte para o suporte técnico.

Antes de começar

Você precisa ter acesso ao pacote de suporte para enviá-lo ao suporte técnico.

Você precisa ter um número de protocolo gerado por meio do site de suporte técnico.

Passos

1. Faça login no site de suporte da NetApp.
2. Carregue o arquivo.

   "Como enviar um arquivo para a NetApp"

Tarefas e informações relacionadas a diversos fluxos de trabalho

Entenda a disputa de componentes de cluster no Active IQ Unified Manager

Você pode identificar problemas de desempenho no cluster quando um componente entra em contenção. O desempenho das cargas de trabalho que usam o componente diminui, e o tempo de resposta (latência) às solicitações do cliente aumenta, o que aciona um evento no Unified Manager.

Um componente que está em contenção não consegue operar em seu nível ideal. Seu desempenho diminuiu, e o desempenho de outros componentes e cargas de trabalho do cluster, chamados de *vítimas*, pode ter aumentado a latência. Para tirar um componente da contenção, é necessário reduzir sua carga de trabalho ou aumentar sua capacidade de lidar com mais trabalho, para que o desempenho retorne 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 storage pode estar sob contenção 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 afetadas, causando queda no desempenho. Para reduzir a quantidade de atividade no agregado, há diferentes medidas que você pode tomar, 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 sofram mais limitação.

O Unified Manager monitora os seguintes componentes do cluster para alertar você quando eles estiverem em contenção:

- **Rede**

  Representa o tempo de espera das solicitações de E/S pelos protocolos de rede externos no cluster. O tempo de espera é o tempo gasto aguardando a conclusão das transações “transfer ready” antes que o cluster possa responder a uma solicitação de E/S. Se o componente de rede estiver em contenção, isso significa que um alto tempo de espera na camada de protocolo está impactando a latência de uma ou mais cargas de trabalho.

- **Processamento de rede**

  Representa o componente de software no cluster envolvido no processamento de E/S entre a camada de protocolo e o cluster. O nó responsável pelo processamento de 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 ativo-ativo, o valor da latência de processamento de rede é exibido para ambos os nós, para que você possa verificar se os nós estão compartilhando a carga igualmente.

- **Limite máximo de QoS**

  Representa a configuração de taxa de transferência máxima (pico) do grupo de políticas de Qualidade de Serviço (QoS) de storage 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 têm a taxa limitada pelo limite de taxa de transferência definido, o que afeta a latência de uma ou mais dessas cargas de trabalho.

- **Limite mínimo de QoS**

  Representa a latência para uma carga de trabalho causada pela configuração mínima (esperada) de taxa de transferência de QoS atribuída a outras cargas de trabalho. Se a configuração mínima de QoS em determinadas cargas de trabalho utilizar a maior parte da largura de banda para garantir a taxa de transferência prometida, outras cargas de trabalho terão sua largura de banda limitada e apresentarão maior latência.

- **Interconexão de cluster**

Representa os cabos e adaptadores com os quais os nós em cluster estão fisicamente conectados. Se o componente de interconexão de cluster estiver em disputa, isso significa que o alto tempo de espera para solicitações de E/S na interconexão de 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 storage que contém a carga de trabalho. O nó que lida com 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 por Volume**

  Representa o processo que monitora o uso de todos os volumes ativos. Em ambientes de grande porte, com mais de 1000 volumes ativos, esse processo monitora quantos volumes críticos precisam acessar recursos por meio do nó simultaneamente. Quando o número de volumes ativos simultâneos excede o limite máximo recomendado, alguns dos volumes não críticos apresentarão latência conforme identificado aqui.

- **MetroCluster Recursos**

  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 do MetroCluster estiver em contenção, isso significa que uma alta taxa de transferência de gravação das cargas de trabalho no cluster local ou um problema na integridade do link está afetando a latência de uma ou mais cargas de trabalho no cluster local. Se o cluster não estiver em uma configuração do MetroCluster, este ícone não será exibido.

- **Operações de agregado ou agregado SSD**

  Representa o agregado de storage no qual as cargas de trabalho estão em execução. Se o componente de 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 em uma combinação de HDDs e SSDs (um agregado Flash Pool), ou em uma combinação de HDDs e uma camada de nuvem (um agregado FabricPool). Um “SSD Aggregate” consiste em todos os SSDs (um agregado all-flash), ou em uma combinação de SSDs e uma camada de nuvem (um agregado FabricPool).

- **Latência na nuvem**

  Representa o componente de software no cluster envolvido no processamento de E/S entre o cluster e a camada de nuvem na qual os dados de usuário são armazenados. Se o componente de latência da nuvem estiver em contenção, isso significa que uma grande quantidade de leituras de volumes hospedados na camada de nuvem está afetando a latência de uma ou mais cargas de trabalho.

- **Sincronização do SnapMirror**

  Representa o componente de software no cluster envolvido na replicação de dados de usuário do volume primário para o volume secundário em uma relação síncrona do SnapMirror. Se o componente de sincronização do SnapMirror estiver em contenção, isso significa que a atividade das operações síncronas do SnapMirror está afetando a latência de uma ou mais cargas de trabalho.

Consulte a página de detalhes de Volume/Saúde em Active IQ Unified Manager

Você pode usar a página de detalhes Volume/Integridade para visualizar informações detalhadas sobre um volume selecionado, como capacidade, eficiência de storage, configuração, proteção, anotação e eventos gerados. Você também pode visualizar informações sobre os objetos relacionados e os alertas relacionados a esse volume.

Você precisa ter a função de Application Administrator ou Storage Administrator.

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 navegar até a página de detalhes de Volume / Performance.

- **Ações**
  - Adicionar alerta

    Permite adicionar um alerta ao volume selecionado.

  - Editar limites

    Permite modificar as configurações de limite para o volume selecionado.

  - Anotar

    Permite adicionar anotações ao volume selecionado.

  - Proteger

    Permite que você crie relacionamentos do SnapMirror ou do SnapVault para o volume selecionado.

  - Relação

    Permite executar as seguintes operações de relacionamento de proteção:

    - Editar

      Abre a caixa de diálogo Editar Relacionamento, que permite alterar as políticas do SnapMirror, os cronogramas e as taxas máximas de transferência existentes para um relacionamento de proteção já em andamento.

    - Abortar

      Interrompe as transferências em andamento de um relacionamento selecionado. Opcionalmente, permite remover o ponto de verificação de reinício para transferências que não sejam a transferência completa. Não é possível remover o ponto de verificação de uma transferência completa.

    - Suspender

      Desativa temporariamente as atualizações agendadas para um relacionamento selecionado. As

transferências que já estão em andamento devem ser concluídas antes que o relacionamento seja colocado em quiesce.

- Interromper

  Rompe a relação entre os volumes de origem e destino e altera o destino para um volume de leitura e gravação.

- Remover

  Exclui permanentemente a relação entre a origem e o destino selecionados. Os volumes não são destruídos, e as cópias Snapshot nos volumes não são removidas. Esta operação não pode ser desfeita.

- Retomar

  Permite transferências agendadas para um relacionamento inativo. No próximo intervalo de transferência agendada, um ponto de verificação de reinicialização será usado, se existir.

- Ressincronizar

  Permite ressincronizar um relacionamento previamente rompido.

- Inicializar/Atualizar

  Permite realizar uma transferência completa em um novo relacionamento de proteção ou uma atualização manual caso o relacionamento já esteja inicializado.

- Ressincronização reversa

  Permite que você restabeleça uma relação de proteção previamente interrompida, invertendo a função da origem e do destino ao tornar a origem uma cópia do destino original. O conteúdo da origem é sobrescrito pelo conteúdo do destino, e todos os dados mais recentes do que os dados na cópia Snapshot comum são excluídos.

◦ Restaurar

Permite restaurar dados de um volume para outro volume. Para obter mais informações, consulte "Restaurando dados usando a página de detalhes de Volume / Integridade".

> O botão Restore e os botões de operação Relationship não estão disponíveis para volumes que estão em relacionamentos de proteção síncrona.

- **Ver volumes**

  Permite navegar até a visualização Health: All Volumes.

Aba Capacidade

A aba 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 Snapshot

  Exibe o espaço de dados consumido pelas cópias Snapshot.

- Usado

  Exibe o espaço utilizado pelos dados no volume.

- Aviso

  Indica que o espaço no volume está quase cheio. Se esse limite for ultrapassado, o sistema gera o evento "Espaço Quase Cheio".

- Erro

  Indica que o espaço no volume está cheio. Se esse limite for ultrapassado, o evento Space Full é gerado.

- Inutilizável

  Indica que o evento "Espaço em Risco no Volume com Provisionamento Dinâmico" foi gerado e que o espaço no volume com provisionamento dinâmico está em risco devido a problemas de capacidade do agregado. A capacidade inutilizável é exibida apenas para volumes com provisionamento dinâmico.

- Gráfico de dados

  Exibe a capacidade total de dados e a capacidade de dados utilizada do volume.

  Se o crescimento automático estiver ativado, o gráfico de dados também exibirá o espaço disponível no agregado. O gráfico de dados exibe o espaço de storage 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 Autogrow está desativado.
    - O volume com crescimento automático ativado atingiu o tamanho máximo.
    - O volume com provisionamento thick e crescimento automático ativado não pode aumentar mais.
  - Capacidade de dados do volume após considerar o tamanho máximo do volume (para volumes com provisionamento thin e para volumes com provisionamento thick 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 espesso que possuem um limite percentual de crescimento automático)

- Gráfico de cópias Snapshot

  Este gráfico é exibido somente quando a capacidade de Snapshot utilizada ou a reserva do Snapshot não for 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 do espaço lógico do volume. O espaço lógico indica o tamanho real dos dados armazenados em disco, sem aplicar as economias obtidas com o uso das tecnologias de eficiência de storage do ONTAP.

  - Relatórios de espaço lógico

    Exibe se o volume tem o relatório de espaço lógico configurado. 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 oferecem suporte ao relatório de espaço lógico.

  - Usado

    Exibe a quantidade de espaço lógico usada pelos dados no volume e a porcentagem de espaço lógico usada com base na capacidade total de dados.

  - Imposição de Espaço Lógico

    Exibe se a imposição de espaço lógico está configurada para volumes com thin provisioning. Quando definida como ativada, o tamanho lógico usado do volume não pode ser maior que o tamanho físico do volume atualmente definido.

- **Crescimento automático**

  Exibe se o volume aumenta automaticamente quando fica sem espaço.

- **Garantia de espaço**

  Exibe o controle de configuração do volume FlexVol quando um volume remove blocos livres de um agregado. Esses blocos passam a ter a garantia de estarem disponíveis para gravações em arquivos no volume. A garantia de espaço pode ser definida para um dos seguintes valores:

  - Nenhum

    Não há garantia de espaço 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 de 100 MB ou mais, a garantia mínima de espaço será definida como 100 MB por padrão. Se o tamanho do volume FlexCache for inferior a 100 MB, a garantia mínima de espaço será definida como o tamanho do volume FlexCache. Se o tamanho do volume FlexCache aumentar posteriormente, a garantia mínima de espaço não será incrementada.

    A garantia de espaço é parcial quando o volume é do tipo Data-Cache.

- **Detalhes (Físico)**

  Exibe as características físicas do volume.

- **Capacidade Total**

  Exibe a capacidade física total no volume.

- **Capacidade de dados**

  Exibe a quantidade de espaço físico utilizado pelo volume (capacidade utilizada) e a quantidade de espaço físico ainda disponível (capacidade livre) no volume. Esses valores também são exibidos como uma porcentagem da capacidade física total.

  Quando o evento "Espaço em risco do volume com provisionamento dinâmico" é gerado para volumes com provisionamento dinâmico, a quantidade de espaço usada pelo volume (capacidade usada) e a quantidade de espaço disponível no volume mas que não pode ser usada (capacidade inutilizável) devido a problemas de capacidade do agregado são exibidas.

- **reserva do Snapshot**

  Exibe a quantidade de espaço usada pelas cópias Snapshot (capacidade utilizada) e a quantidade de espaço disponível para as cópias Snapshot (capacidade livre) no volume. Esses valores também são exibidos como uma porcentagem da reserva total do Snapshot.

  Quando o evento "Thin-Provisioned Volume Space At Risk" é gerado para volumes com provisionamento dinâmico, são exibidos a quantidade de espaço usada pelas cópias Snapshot (capacidade utilizada) e o volume de espaço disponível no volume, mas que não pode ser usado para criar cópias Snapshot (capacidade inutilizável) devido a problemas de capacidade do agregado.

- **Limiares de Volume**

  Exibe os seguintes limites de capacidade de volume:

  - Limiar de quase cheio

    Especifica a porcentagem em que um volume está quase cheio.

  - Limiar total

    Especifica a porcentagem em que um volume está cheio.

- **Outros detalhes**

  - Tamanho máximo de crescimento automático

    Exibe o tamanho máximo que o volume pode atingir automaticamente. O valor padrão é 120% do tamanho do volume no momento da criação. Este campo é exibido somente quando o crescimento automático está ativado para o volume.

  - Capacidade comprometida da cota Qtree

    Exibe o espaço reservado nas cotas.

  - Capacidade de superalocação da cota de 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 por cento do espaço reservado necessário é reservado para que os objetos fiquem totalmente protegidos contra sobrescritas. Se a reserva fracionária for menor que 100 por cento, o espaço reservado para todos os arquivos com espaço reservado nesse volume será reduzido à porcentagem da reserva fracionária.

- Taxa de crescimento diária do Snapshot

  Exibe a variação (em porcentagem, KB, MB, GB etc.) que ocorre a cada 24 horas nas cópias Snapshot no volume selecionado.

- Dias até a capacidade total do Snapshot

  Exibe o número estimado de dias restantes antes que o espaço reservado para as cópias Snapshot no volume atinja o limite especificado.

  O campo "Snapshot Days to Full" exibe o valor "Not Applicable" quando a taxa de crescimento das cópias Snapshot no volume é zero ou negativa, ou quando não há dados suficientes para calcular a taxa de crescimento.

- O Snapshot Autodelete

  Especifica se as cópias Snapshot são excluídas automaticamente para liberar espaço livre quando uma gravação em um volume falha devido à falta de espaço no agregado.

- Cópias Snapshot

  Exibe informações sobre as cópias Snapshot no volume.

  O número de cópias Snapshot no volume é exibido como um link. Clicar no link abre a caixa de diálogo "Snapshot Copies on a Volume", que exibe detalhes das cópias Snapshot.

A contagem de cópias Snapshot é atualizada aproximadamente a cada hora; no entanto, a lista de cópias Snapshot é atualizada no momento em que você clica no ícone. Isso pode resultar em uma diferença entre a contagem de cópias Snapshot exibida na topologia e o número de cópias Snapshot listadas quando você clica no ícone.

- **Volume Move**

  Exibe o status da operação atual de movimentação de volume ou da última operação realizada no volume, além de outros detalhes, como a fase atual da operação de movimentação de volume em andamento, agregado de origem, agregado de destino, a hora de início, a hora de término e a hora de término estimada.

  Exibe também o número de operações de movimentação de volume realizadas no volume selecionado. Você pode visualizar mais informações sobre as operações de movimentação de volume clicando no link **Histórico de Movimentação de Volume**.

Guia de configuração

A aba 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 storage 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 tiering

    Exibe a política de armazenamento em camadas definida para o volume, se o volume estiver implantado em um agregado habilitado para o FabricPool. A política pode ser None, Snapshot Only, Backup, Auto ou All.

  - VM de armazenamento

    Exibe o nome da SVM que contém o volume.

  - Caminho de Junção

    Exibe o status do caminho, que pode estar ativo ou inativo. O caminho na SVM em que o volume está montado também é exibido. Você pode clicar no link **Histórico** para visualizar as cinco alterações mais recentes no caminho de junção.

  - Política de exportação

    Exibe o nome da política de exportação criada para o volume. Você pode clicar no link para ver detalhes sobre as políticas de exportação, os protocolos de autenticação e o acesso habilitado nos volumes que pertencem ao SVM.

  - Estilo

    Exibe o estilo de volume. O estilo de volume pode ser o FlexVol ou o 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 de RAID pode ser RAID0, RAID4, RAID-DP ou RAID-TEC.

    Vários tipos de RAID podem ser exibidos para os volumes FlexGroup porque os volumes constituintes dos FlexGroups podem estar em agregados de tipos diferentes.

- SnapLock Tipo

  Exibe o tipo de SnapLock do agregado que contém o volume.

- SnapLock Expiração

  Exibe a data de validade do volume de SnapLock.

- **Capacidade**
  - Thin provisioning

    Exibe se o thin provisioning está configurado para o volume.

  - Crescimento automático

    Exibe se o volume flexível cresce automaticamente dentro de um agregado.

  - O Snapshot Autodelete

    Especifica se as cópias Snapshot são excluídas automaticamente para liberar espaço livre quando uma gravação em um volume falha devido à falta de espaço no agregado.

  - Cotas

    Especifica se as quotas estão ativadas para o volume.

- **Eficiência**
  - Compressão

    Especifica se a compressão está ativada ou desativada.

  - Desduplicação

    Especifica se a desduplicação está ativada ou desativada.

  - Modo de desduplicação

    Especifica se a operação de deduplicação habilitada em um volume é manual, agendada ou baseada em políticas. Se o modo estiver definido como agendado, a programação da operação será exibida, e se o modo estiver definido como baseado em políticas, o nome da política será exibido.

  - Tipo de desduplicação

    Especifica o tipo de operação de deduplicação em execução no volume. Se o volume estiver em uma relação do SnapVault, o tipo exibido será SnapVault. Para qualquer outro volume, o tipo exibido será Regular.

  - Política de Eficiência de Armazenamento

    Especifica o nome da política de eficiência de storage que foi atribuída a este volume por meio do Unified Manager. Essa política pode controlar as configurações de compactação e deduplicação.

- **Proteção**
  - Cópias Snapshot

Especifica se as cópias Snapshot automáticas estão ativadas ou desativadas.

Aba de proteção

A aba Proteção exibe detalhes de proteção do volume selecionado, como informações de atraso, tipo de relação e topologia da relação.

- **Resumo**

  Exibe as propriedades das relações de proteção (SnapMirror, SnapVault ou DR de VM de storage) de um volume selecionado. Para qualquer outro tipo de relação, somente a propriedade Tipo de relação é exibida. Se um volume primário for selecionado, somente as políticas de cópia Snapshot Gerenciado e Snapshot Local serão exibidas. As propriedades exibidas para as relações de 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 do lag

    Exibe o status de atraso na atualização ou transferência de uma relação de proteção. O status pode ser Erro, Aviso ou Crítico.

    O status de atraso não se aplica a relacionamentos síncronos.

  - Duração do atraso

    Exibe o tempo de atraso dos dados no espelho em relação à origem.

  - Última atualização bem-sucedida

    Exibe a data e a hora da atualização de proteção mais recente concluída com sucesso.

    A última atualização bem-sucedida não se aplica a relacionamentos síncronos.

  - Membro do Serviço de Armazenamento

    Exibe "Sim" ou "Não" para indicar se o volume pertence a um serviço de armazenamento e é gerenciado por ele.

  - Replicação flexível de versão

    Exibe Sim, Sim com opção de backup ou Nenhum. Sim indica que a replicação do SnapMirror é possível mesmo que os volumes de origem e destino estejam executando versões diferentes do software ONTAP. Sim com opção de backup indica a implementação da proteção do SnapMirror com a capacidade de reter 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 do ONTAP disponíveis para a relação de proteção.

  - Serviço de proteção

    Exibe o nome do serviço de proteção se um aplicativo parceiro de proteção gerenciar o

relacionamento.

- Tipo de relacionamento

  Exibe qualquer tipo de relacionamento, incluindo Espelhamento assíncrono, Cofre assíncrono, MirrorVault assíncrono, StrictSync e Sync.

- Estado do relacionamento

  Exibe o estado da relação do SnapMirror ou do SnapVault. O estado pode ser Não inicializado, SnapMirrored ou Desconectado. Se um volume de origem for selecionado, o estado da relação não se aplica e não é exibido.

- Status da transferência

  Exibe o status da transferência da relação de proteção. O status da transferência pode ser um dos seguintes:

  - Abortando

    As transferências do SnapMirror estão habilitadas; no entanto, uma operação de cancelamento 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 não há transferência em andamento.

  - Finalizando

    As transferências do SnapMirror estão habilitadas. Atualmente, o volume está na fase pós-transferência para transferências incrementais do SnapVault.

  - Inativo

    As transferências estão ativadas e nenhuma transferência está em andamento.

  - Em sincronia

    Os dados nos dois volumes na relação síncrona estão sincronizados.

  - Fora de sincronia

    Os dados no volume de destino não estão sincronizados com o volume de origem.

  - Preparando

    As transferências do SnapMirror estão habilitadas. O volume está atualmente na fase de pré-transferência para transferências incrementais do SnapVault.

  - Em fila

    As transferências do SnapMirror estão ativadas. Nenhuma transferência está em andamento.

  - Em estado inativo

As transferências do SnapMirror estão desativadas. Nenhuma transferência está em andamento.

- Colocando em quiescência

  Uma transferência do SnapMirror está em andamento. As transferências adicionais estão desativadas.

- Transferindo

  As transferências do SnapMirror estão ativadas e uma transferência está em andamento.

- Em transição

  A transferência assíncrona de dados da 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 colocadas na fila.

◦ Taxa máxima de transferência

Exibe a taxa de transferência máxima da relação. A taxa de transferência máxima pode ser um valor numérico em kilobytes por segundo (Kbps), Megabytes por segundo (Mbps), Gigabytes por segundo (Gbps) ou Terabytes por segundo (Tbps). Se "No Limit" for exibido, a transferência completa entre as relações será ilimitada.

◦ Política do SnapMirror

Exibe a política de proteção do volume. DPDefault indica a política de proteção padrão de espelhamento assíncrono, XDPDefault indica a política padrão de Vault assíncrono, e DPSyncDefault indica a política padrão de MirrorVault assíncrono. StrictSync indica a política de proteção Strict síncrona padrão, e Sync indica a política síncrona padrão. Você pode clicar no nome da política para ver os detalhes associados a essa política, incluindo as seguintes informações:

- Prioridade de transferência
- Ignorar configuração de tempo de acesso
- Limite de tentativas
- Comentários
- Rótulos do SnapMirror
- Configurações de retenção
- Cópias Snapshot reais
- Preservar cópias Snapshot
- Limiar de aviso de retenção
- Cópias Snapshot sem configurações de retenção. Em uma relação do SnapVault em cascata na qual a origem é um volume de proteção de dados (DP), somente a regra “sm_created” se aplica.

◦ Cronograma de atualização

Exibe o agendamento do SnapMirror atribuído ao relacionamento. Ao posicionar o cursor sobre o ícone de informações, você vê os detalhes do agendamento.

- Política de Snapshot local

  Exibe a política de cópia Snapshot para o volume. A política é "Default", "None" ou qualquer nome atribuído a uma política personalizada.

- Protegido por

  Exibe o tipo de proteção usado para o volume selecionado. Por exemplo, se um volume estiver protegido por um Grupo de consistência e por relacionamentos de volume do SnapMirror, este campo exibirá tanto o SnapMirror quanto o Grupo de consistência. Este campo também fornece um link que redireciona você para a página Relationships para ver o status unificado do relacionamento. O link se aplica apenas a relacionamentos constituintes.

- Grupo de consistência

  Para volumes protegidos por relacionamentos de sincronização ativa 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 relação de proteção. A direção das relações na topologia é exibida da esquerda para a direita, com a origem de cada relação à esquerda e o destino à direita.

  Duas linhas em negrito especificam uma relação de Mirror assíncrono, uma única linha em negrito especifica uma relação de Vault assíncrono, duas linhas simples especificam uma relação de MirrorVault assíncrono, e uma linha em negrito e uma linha sem negrito especificam uma relação síncrona. A tabela abaixo indica se a relação síncrona é StrictSync ou Sync.

  Clicar com o botão direito do mouse em um volume exibe um menu no qual você pode escolher proteger o volume ou restaurar dados para ele. Clicar com o botão direito do mouse em uma relação exibe um menu no qual você pode escolher editar, abortar, suspender, interromper, remover ou retomar a relação.

  Os menus não serão exibidos nos seguintes casos:

  - Se as configurações do RBAC não permitirem essa ação, por exemplo, se você tiver apenas privilégios de operador
  - Se o volume estiver em uma relação de proteção síncrona
  - Quando o ID do volume é desconhecido, por exemplo, quando você tem uma relação de intercluster e o cluster de destino ainda não foi descoberto, clicar em outro volume na topologia seleciona e exibe informações desse volume. Um ponto de interrogação () no canto superior esquerdo de um volume indica que o volume está ausente ou que ainda não foi descoberto. Isso também pode indicar que as informações de capacidade estão ausentes. Posicionar o cursor sobre o ponto de interrogação exibe informações adicionais, incluindo sugestões de ação corretiva.

  A topologia exibe informações sobre a capacidade do volume, o atraso, as cópias Snapshot e a última transferência de dados bem-sucedida, se estiver em conformidade com um dos vários modelos de topologia comuns. Se uma topologia não estiver em conformidade com um desses modelos, as informações sobre o atraso do volume e a última transferência de dados bem-sucedida serão exibidas em uma tabela de relacionamento abaixo da topologia. Nesse caso, a linha destacada na tabela indica o volume selecionado e, na visualização da topologia, 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. Ao posicionar o cursor sobre um volume na topologia, você vê as configurações atuais de limite de aviso e crítico desse volume na caixa de diálogo Configurações atuais de limite. Você também pode editar as configurações de limite clicando no link **Editar limites** na caixa de diálogo Configurações atuais de limite. Desmarcar a caixa de seleção **Capacidade** oculta todas as informações de capacidade de todos os volumes na topologia.

- Atraso

  Exibe a duração e o status do atraso das relações de proteção de entrada. Desmarcar a caixa de seleção **Atraso** oculta todas as informações de atraso de todos os volumes na topologia. Quando a caixa de seleção **Atraso** está esmaecida, as informações de atraso do volume selecionado são exibidas na tabela de relacionamentos abaixo da topologia, bem como as informações de atraso de todos os volumes relacionados.

- Snapshot

  Exibe o número de cópias Snapshot disponíveis para um volume. Desmarcar a caixa de seleção **Snapshot** oculta todas as informações de cópia Snapshot de todos os volumes na topologia. Clicar em um ícone de cópia Snapshot () exibe a lista de cópias Snapshot de um volume. A contagem de cópias Snapshot exibida ao lado do ícone é atualizada aproximadamente a cada hora; no entanto, a lista de cópias Snapshot é atualizada no momento em que você clica no ícone. Isso pode resultar em uma diferença entre a contagem de cópias Snapshot exibida na topologia e o número de cópias Snapshot listadas quando você clica no ícone.

- Última transferência bem-sucedida

  Exibe a quantidade, a duração, a hora e a data da última transferência de dados. Quando a caixa de seleção **Última Transferência Bem-Sucedida** estiver esmaecida, as informações da última transferência bem-sucedida do volume selecionado são exibidas na tabela de relacionamento abaixo da topologia, bem como as informações da última transferência bem-sucedida de 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 da defasagem do relacionamento de entrada, duração da transferência do relacionamento de entrada e tamanho da transferência do relacionamento de entrada. As informações de histórico são exibidas somente quando você seleciona um volume de destino. Se você selecionar um volume primário, os gráficos ficarão vazios e a mensagem "No data found" será exibida. Se os volumes estiverem protegidos por relacionamentos síncronos de Consistency Group e 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 History. Você também pode ver detalhes de um período 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 o limite de erro de atraso estiver sendo ultrapassado de forma consistente, você pode tomar a medida apropriada. Além disso, você pode clicar no botão **Export** para criar um relatório em formato CSV para o gráfico que 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 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. Ao posicionar o cursor sobre essas linhas, você visualiza a configuração do limite. A linha horizontal azul 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 do relacionamento**

  Exibe segundos, minutos ou horas no eixo vertical (y) e dias, meses ou anos no eixo horizontal (x), dependendo do período de duração selecionado. O valor superior no eixo y indica a duração máxima da 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 estejam em relações de proteção síncrona.

- **Tamanho Transferido do Relacionamento**

  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 tempo 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 estejam em relações de proteção síncrona.

Área de histórico

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 **Export** para criar um relatório em formato CSV para o gráfico que 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 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 Nearly Full, você poderá tomar a medida apropriada.

Os gráficos de histórico exibem as seguintes informações:

- **Capacidade do 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 linha em bytes, kilobytes, megabytes e assim por diante, no eixo vertical (y). O período é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode ver os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma determinada área. Você pode ocultar ou exibir um gráfico de linha clicando na legenda

apropriada. Por exemplo, quando você clica na legenda Volume Used Capacity, a linha do gráfico Volume Used Capacity fica oculta.

- **Capacidade do volume usada 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 da desduplicação e da compactação, como gráficos de linhas, em bytes, kilobytes, megabytes e assim por diante, no eixo vertical (y). O período é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode ver 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 "Trend Capacity Used", a linha do gráfico Trend Capacity Used fica oculta.

- **Capacidade do volume usada (%)**

  Exibe a capacidade usada no volume e a tendência de como a capacidade do volume é usada com base no histórico de uso, como gráficos de linhas, em porcentagem, no eixo vertical (y). O período é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode ver os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma determinada área. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda apropriada. Por exemplo, ao clicar na legenda "Volume Used Capacity", a linha do gráfico "Volume Used Capacity" é ocultada.

- **Capacidade de Snapshot usada (%)**

  Exibe a reserva do Snapshot e o limite de aviso do Snapshot como gráficos de linhas, e a capacidade usada pelas cópias Snapshot como um gráfico de área, em porcentagem, no eixo vertical (y). A sobrecarga do Snapshot é representada com cores diferentes. O período é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode ver os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma determinada área. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda correspondente. Por exemplo, ao clicar na legenda Reserva do Snapshot, a linha do gráfico Reserva do Snapshot 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.

- **Hora de acionamento**

  Exibe o tempo decorrido desde que o evento foi gerado. Se o tempo decorrido for superior a uma semana, o carimbo de data/hora em que o evento foi gerado será exibido.

Painel de anotações relacionadas

O painel Anotações Relacionadas permite visualizar detalhes das anotações associadas ao volume selecionado. Os detalhes incluem o nome da anotação e os valores de anotação aplicados ao volume. Você também pode remover anotações manuais do painel Anotações Relacionadas.

Painel de dispositivos relacionados

O painel Dispositivos Relacionados permite visualizar e navegar até as SVMs, agregados, qtrees, LUNs e cópias Snapshot relacionadas ao volume:

- **Máquina virtual de armazenamento**

  Exibe a capacidade e o estado de integridade da SVM que contém o volume selecionado.

- **Agregado**

  Exibe a capacidade e o estado de integridade do agregado que contém o volume selecionado. Para volumes FlexGroup, o número de agregados que compõem o FlexGroup é listado.

- **Volumes no agregado**

  Exibe o número e a capacidade de todos os volumes que pertencem ao agregado pai do volume selecionado. O estado de 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 de Aviso e os cinco restantes exibem o status Crítico, o status exibido será Crítico. Este componente não aparece para volumes FlexGroup.

- **Qtrees**

  Exibe o número de qtrees que o volume selecionado contém e a capacidade de qtrees com cota que o volume selecionado contém. A capacidade de qtrees com cota é exibida em relação à capacidade de dados do volume. O status de integridade 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 as cinco restantes com status Crítico, o status exibido será Crítico.

- **Compartilhamentos NFS**

  Exibe o número e o status dos compartilhamentos NFS associados ao volume.

- **Compartilhamentos SMB**

  Exibe o número e o status dos compartilhamentos SMB/CIFS.

- **LUNs**

  Exibe o número e o tamanho total de todos os LUNs no volume selecionado. O estado de integridade dos LUNs também é exibido, com base no nível de gravidade mais alto.

- **Cotas de usuários e grupos**

  Exibe o número e o status das quotas de usuário e de grupo de usuários associadas ao volume e às suas qtrees.

- **Volumes FlexClone**

  Exibe o número e a capacidade de todos os volumes clonados do volume selecionado. O número e a capacidade são exibidos somente se o volume selecionado contiver algum volume clonado.

- **Volume pai**

  Exibe o nome e a capacidade do volume pai de um volume FlexClone selecionado. O volume pai é exibido

somente se o volume selecionado for um volume FlexClone.

Painel de Grupos Relacionados

O painel Grupos Relacionados permite visualizar a lista de grupos associados ao volume selecionado.

Painel de alertas relacionados

O painel Alertas Relacionados permite visualizar a lista de alertas criados para o volume selecionado. Você também pode adicionar um alerta clicando no link Adicionar Alerta ou editar um alerta existente clicando no nome do alerta.

Visualize a página de detalhes de VM de armazenamento/saúde no Active IQ Unified Manager

Você pode usar a página Detalhes da VM de storage / Integridade para visualizar informações detalhadas sobre a VM de storage selecionada, como sua integridade, capacidade, configuração, políticas de dados, interfaces lógicas (LIFs), LUNs, qtrees, cotas de usuários e grupos de usuários e detalhes de proteção. Você também pode visualizar informações sobre os objetos relacionados e os alertas relacionados à VM de storage.

Você pode monitorar apenas a VM de storage 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 navegar até a página de detalhes de desempenho da VM de storage.

- **Ações**
  - Adicionar alerta

    Permite adicionar um alerta à máquina virtual de armazenamento selecionada.

  - Anotar

    Permite adicionar anotações à VM de storage selecionada.

- **Visualizar VMs de armazenamento**

  Permite navegar até a visualização "Saúde: todas as VMs de storage".

Aba Saúde

A aba 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 do volume que exibe avisos para visualizar a lista de volumes que apresentam

problemas de capacidade com gravidade de aviso.

- **Problemas de disponibilidade**

  Exibe, em forma de gráfico, o número total de objetos, incluindo aqueles com problemas de disponibilidade e aqueles sem problemas relacionados à disponibilidade. As cores no gráfico representam os diferentes níveis de gravidade dos problemas. As informações abaixo do gráfico fornecem detalhes sobre os problemas de disponibilidade que podem afetar ou já afetaram a disponibilidade dos dados na VM de storage. Por exemplo, exibe informações sobre as LIFs NAS e SAN que estão inativas e os volumes que estão offline.

  Você também pode visualizar informações sobre os protocolos e serviços relacionados que estão em execução no momento, bem como o número e o status dos compartilhamentos NFS e CIFS.

- **Problemas de capacidade**

  Exibe, em forma de gráfico, o número total de objetos, incluindo objetos com problemas de capacidade e objetos sem problemas relacionados à capacidade. As cores no gráfico representam os diferentes níveis de gravidade dos problemas. As informações abaixo do gráfico fornecem detalhes sobre problemas de capacidade que podem afetar ou já afetaram a capacidade dos dados na VM de storage. Por exemplo, exibe informações sobre agregados que provavelmente ultrapassarão os valores de limite definidos.

- **Problemas de proteção**

  Fornece uma visão geral rápida da integridade relacionada à proteção da VM de storage, exibindo, em uma caixa de diálogo de campo, o número total de relações, incluindo relações que têm problemas de proteção e relações que não têm nenhum problema relacionado à proteção. Você também pode ver o status da relação de DR da VM de storage da VM de storage selecionada. Os eventos das relações de DR da VM de storage são exibidos aqui, e clicar nos eventos leva você para a página de detalhes do evento. Quando existem volumes desprotegidos, clicar no link leva você para a visualização "Integridade: todos os volumes", em que você pode ver uma lista filtrada dos volumes desprotegidos na VM de storage. As cores no gráfico representam os diferentes níveis de gravidade dos problemas. Clicar em um gráfico leva você para a visualização "Relação: todas as relações", em que você pode ver uma lista filtrada dos detalhes da relação de proteção. As informações abaixo do gráfico fornecem detalhes sobre problemas de proteção que podem afetar ou já afetaram a proteção dos dados na VM de storage. Por exemplo, são exibidas informações sobre volumes que têm uma reserva de cópia Snapshot quase cheia ou sobre problemas de atraso na relação do SnapMirror.

Aba Capacidade

A aba Capacidade exibe informações detalhadas sobre a capacidade de dados da SVM selecionada.

As seguintes informações são exibidas para uma Storage VM com FlexVol volume ou FlexGroup volume:

- **Capacidade**

  A área de capacidade exibe detalhes sobre a capacidade utilizada 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.

- Disponibilidade garantida

  Exibe o espaço disponível garantido para dados que está disponível para volumes na Storage VM.

- Não garantido

  Exibe o espaço disponível restante para os dados alocados aos volumes com thin provisioning na Storage VM.

- **Volumes com problemas de capacidade**

A lista de volumes com problemas de capacidade exibe, em formato tabular, detalhes sobre os volumes que apresentam problemas de capacidade:

- Status

  Indica que o volume apresenta um problema relacionado à capacidade, com a gravidade indicada.

  Você pode mover o ponteiro sobre o status para visualizar mais informações sobre os eventos relacionados à capacidade 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 data e a hora em que o evento foi acionado, o nome do administrador ao qual o evento está atribuído e a causa do evento. Você pode usar o botão **Exibir detalhes** para ver mais informações sobre o evento.

  Se o status do volume for determinado por vários eventos da mesma gravidade, os três principais eventos serão exibidos com informações como o nome do evento, a hora e a data em que os eventos foram acionados e o nome do administrador ao qual o evento está atribuído. Você pode visualizar 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. No entanto, apenas a gravidade mais alta é exibida. Por exemplo, se um volume tiver dois eventos com gravidades de Erro e Aviso, apenas a gravidade de Erro é exibida.

- Volume

  Exibe o nome do volume.

- Capacidade de dados utilizada

  Exibe, em forma de gráfico, informações sobre a utilização da capacidade do volume (em porcentagem).

- Dias até encher

  Exibe o número estimado de dias restantes antes que o volume atinja a capacidade máxima.

- Thin provisioning

  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, seu volume raiz, o tipo de volumes que ela contém (FlexVol volumes), políticas e proteção criadas na VM de armazenamento:

- **Visão geral**
  - Cluster

    Exibe o nome do cluster ao qual a máquina virtual de armazenamento pertence.

  - Tipo de volume permitido

    Exibe o tipo de volumes que podem ser criados na VM de storage. O tipo pode ser FlexVol ou FlexVol/FlexGroup.

  - Volume raiz

    Exibe o nome do volume raiz da VM de storage.

  - Protocolos permitidos

    Exibe os tipos de protocolos que podem ser configurados na VM de armazenamento. Também indica se um protocolo está ativo (), inativo () 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 inativas ().

  - SAN

    Exibe o número de interfaces SAN associadas à VM de armazenamento. Também indica se as interfaces estão ativas () ou inativas ().

  - FC-NVMe

    Exibe o número de interfaces FC-NVMe associadas à VM de armazenamento. Também indica se as interfaces estão ativas () ou inativas ().

- **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 inativas ().

- **Políticas**
  - Instantâneos

Exibe o nome da política do Snapshot criada na Storage VM.

- Políticas de exportação

  Exibe o nome da política de exportação caso apenas uma política tenha sido criada ou o número de políticas de exportação caso várias políticas tenham sido criadas.

- **Proteção**
  - DR de VM de armazenamento

    Exibe se a VM de armazenamento selecionada está protegida, é destino ou não está protegida e o nome do destino no qual a VM de armazenamento está protegida. Se a VM de armazenamento selecionada for 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 à grade de relacionamento de VMs de armazenamento filtrada pela 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 se refere aos volumes de destino da VM de armazenamento selecionada.

  - Volumes não protegidos

    Exibe o número de volumes desprotegidos na máquina virtual de armazenamento selecionada.

- **Serviços**
  - Tipo

    Exibe o tipo de serviço configurado na VM de storage. O tipo pode ser Domain Name System (DNS) ou Network Information Service (NIS).

  - Estado

    Exibe o estado do serviço, que pode ser Ativo ( ), Inativo ( ) 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 ativado, o FQDN ativo do servidor NIS é exibido. Quando o servidor NIS está desativado, a lista de todos os FQDNs é exibida.

  - Endereço IP

    Exibe os endereços IP do servidor DNS ou NIS. Quando o servidor NIS está 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 storage selecionada.

- **Status Operacional**

  Exibe o status operacional da interface, que pode ser Ativo (), Inativo () 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 Up (), Down () ou Unknown (). O status administrativo de uma interface é controlado pelo administrador de storage para fazer alterações na configuração ou para fins de manutenção. O status administrativo pode ser diferente do status operacional. No entanto, se o status administrativo de uma interface for Down, o status operacional será Down por padrão.

- **Endereço IP / WWPN**

  Exibe o endereço IP das interfaces Ethernet e o World Wide Port Name (WWPN) das LIFs FC.

- **Protocolos**

  Exibe a lista de protocolos de dados especificados para a interface, como CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe e FlexCache.

- **Função**

  Exibe a função da interface. As funções podem ser Dados ou Gerenciamento.

- **Porta inicial**

  Exibe a porta física à qual a interface estava 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.

- **Conjunto de portas**

  Exibe o conjunto de portas ao qual a interface está mapeada.

- **Política de Failover**

  Exibe a política de failover configurada para a interface. Para interfaces NFS, CIFS e FlexCache, a política de failover padrão é Next Available. A política de failover não se aplica a interfaces FC e iSCSI.

- **Grupos de Roteamento**

  Exibe o nome do grupo de roteamento. Você pode visualizar mais informações sobre as rotas e o gateway de destino clicando no nome do grupo de roteamento.

  Os grupos de roteamento não são compatíveis com o ONTAP 8.3 ou posterior e, portanto, é exibida uma coluna em branco para esses clusters.

- **Grupo de failover**

  Exibe o nome do grupo de failover.

Aba Qtrees

A aba Qtrees exibe detalhes sobre os qtrees e suas cotas. Você pode clicar no botão **Editar Limiares** se quiser editar as configurações de limite de integridade da 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 de qtrees para a VM de armazenamento atual, para todas as VMs de armazenamento no cluster atual ou para todas as VMs de armazenamento em todos os clusters do seu data center. Alguns campos adicionais de qtrees aparecem no arquivo CSV exportado.

- **Status**

  Exibe o estado atual da qtree. O estado 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 a qtree.

  Se o status da qtree for determinado por um único evento, você poderá visualizar informações como o nome do evento, a data e hora em que o evento foi acionado, o nome do administrador a quem o evento está atribuído e a causa do evento. Você pode usar **Exibir detalhes** para ver mais informações sobre o evento.

  Se o status da qtree for determinado por múltiplos 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 está atribuído. Você pode visualizar mais detalhes sobre cada um desses eventos clicando no nome do evento. Você também pode usar **View All Events** para visualizar a lista de eventos gerados.

  > Uma qtree pode ter múltiplos eventos com a mesma gravidade ou com gravidades diferentes. No entanto, apenas a gravidade mais alta é exibida. Por exemplo, se uma qtree tiver dois eventos com gravidades de Erro e Aviso, apenas a gravidade de Erro será exibida.

- **Qtree**

  Exibe o nome da qtree.

- **Cluster**

  Exibe o nome do cluster que contém a qtree. Aparece apenas no arquivo CSV exportado.

- **Máquina virtual de armazenamento**

  Exibe o nome da máquina virtual de armazenamento (SVM) que contém a qtree. Aparece apenas no arquivo CSV exportado.

- **Volume**

  Exibe o nome do volume que contém a qtree.

Você pode mover o ponteiro sobre o nome do volume para ver mais informações sobre o volume.

- **Conjunto de Cotas**

  Indica se uma quota está ativada ou desativada na qtree.

- **Tipo de quota**

  Especifica se a cota é para um usuário, grupo de usuários ou um qtree. Aparece apenas 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 for qtree ou se a cota não estiver definida, a coluna ficará vazia. Aparece apenas no arquivo CSV exportado.

- **% de disco usado**

  Exibe a porcentagem de espaço de disco usado. Se um limite rígido de disco estiver definido, esse valor será baseado no limite rígido de disco. Se a cota estiver 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, então “Not applicable” será exibido na página da grade, e o campo ficará em branco nos dados de exportação CSV.

- **Limite rígido de disco**

  Exibe a quantidade máxima de espaço de disco alocado para a qtree. O Unified Manager gera um evento crítico quando esse limite é atingido e nenhuma gravação adicional em disco é permitida. O valor é exibido como “Unlimited” nas seguintes condições: se a cota estiver definida sem um limite rígido, se a cota não estiver definida ou se as cotas estiverem desativadas no volume ao qual a qtree pertence.

- **Limite flexível de disco**

  Exibe a quantidade de espaço de disco alocado para a qtree antes que um evento de aviso seja gerado. O valor é exibido como “Ilimitado” nas seguintes condições: se a cota estiver definida sem um limite flexível de disco, se a cota não estiver definida ou se as cotas estiverem desativadas no volume ao qual a qtree pertence. Por padrão, esta coluna fica oculta.

- **Limiar de disco**

  Exibe o valor de limite definido para o espaço de disco. O valor é exibido como “Unlimited” nas seguintes condições: se a cota estiver definida sem um valor limite para espaço em disco, se a cota não estiver definida ou se as cotas estiverem desativadas no volume ao qual o qtree pertence. Por padrão, esta coluna fica oculta.

- **% de arquivos usados**

  Exibe a porcentagem de arquivos usados na qtree. Se o limite rígido de arquivos estiver definido, esse valor será baseado no limite rígido de arquivos. Nenhum valor será exibido se a cota estiver definida sem um limite rígido de arquivos. Se a cota não estiver definida ou se as cotas estiverem desativadas no volume ao qual a qtree pertence, então “Not applicable” será exibido na página da grade e o campo ficará em branco nos dados de exportação CSV.

- **Limite rígido de arquivos**

Exibe o limite rígido para o número de arquivos permitidos nas qtrees. O valor é exibido como “Ilimitado” nas seguintes condições: se a cota estiver definida sem um limite rígido de arquivos, se a cota não estiver 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 nos qtrees. O valor é exibido como “Ilimitado” nas seguintes condições: se a cota estiver definida sem um limite flexível de arquivos, se a cota não estiver definida ou se as cotas estiverem desativadas no volume ao qual o qtree pertence. Por padrão, esta coluna fica oculta.

Aba Cotas de Usuário e Grupo

Exibe detalhes sobre as quotas de usuário e de grupo de usuários da VM de armazenamento selecionada. Você pode visualizar informações como o status da quota, o nome do usuário ou do grupo de usuários, os limites flexíveis e rígidos definidos nos discos e arquivos, a quantidade de espaço de disco e o 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 Edit Email Address, que exibe o endereço de email atual do usuário ou grupo de usuários selecionado. Você pode modificar o endereço de email. Se o campo **Edit Email Address** estiver em branco, a regra padrão será usada para gerar um endereço de email para o usuário ou grupo de usuários selecionado.

  Se mais de um usuário tiver a mesma cota, os nomes dos usuários serão exibidos 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 o envio de notificações.

- **Botão de comando Configurar regras de e-mail**

  Permite criar ou modificar regras para gerar um endereço de e-mail para as quotas de usuário ou de grupo de usuários configuradas na máquina virtual de armazenamento. Uma notificação é enviada para o endereço de e-mail especificado quando ocorre uma violação de quota.

- **Status**

  Exibe o status atual da cota. O status pode ser Crítico (), Aviso () ou Normal ().

  Você pode mover o cursor sobre o ícone de status para visualizar mais informações sobre o evento ou os 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 data e a hora em que o evento foi acionado, o nome do administrador ao qual o evento está atribuído e a causa do evento. Você pode usar **Exibir detalhes** para ver mais informações sobre o evento.

  Se o status da cota for determinado por vários eventos da mesma gravidade, os três principais eventos serão exibidos com informações como o nome do evento, a hora e a data em que os eventos foram acionados e o nome do administrador ao qual o evento está atribuído. Você pode visualizar mais detalhes sobre cada um desses eventos clicando no nome do evento. Você também pode usar **View All Events** para visualizar a lista de eventos gerados.

  Uma cota pode ter vários eventos da mesma gravidade ou de gravidades diferentes. No

entanto, apenas a gravidade mais alta é exibida. Por exemplo, se uma cota tiver dois eventos com gravidades de Erro e Aviso, apenas a gravidade de Erro é exibida.

- **Usuário ou Grupo**

  Exibe o nome do usuário ou grupo de usuários. Se mais de um usuário tiver a mesma cota, os nomes dos usuários serão exibidos como valores separados por vírgula.

  O valor é exibido como “Unknown” quando o ONTAP não fornece um nome de usuário válido devido a erros do SecD.

- **Tipo**

  Especifica se a quota se aplica a um usuário ou a 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 visualizar mais informações sobre o volume ou qtree.

- **% de disco usado**

  Exibe a porcentagem de espaço de disco utilizado. O valor é exibido como “Não aplicável” se a cota for definida sem um limite rígido.

- **Limite rígido de disco**

  Exibe a quantidade máxima de espaço de disco alocado para a cota. O Unified Manager gera um evento crítico quando esse limite é atingido e nenhuma gravação adicional em disco é permitida. O valor é exibido como “Unlimited” se a cota for definida sem um limite rígido de disco.

- **Limite flexível de disco**

  Exibe a quantidade de espaço de disco alocado para a cota antes que um evento de aviso seja gerado. O valor é exibido como “Unlimited” se a cota for definida sem um limite flexível de disco. Por padrão, esta coluna fica oculta.

- **Limiar de disco**

  Exibe o valor de limite definido para o espaço de disco. O valor é exibido como “Unlimited” se a cota estiver definida sem um valor de limite para espaço de disco. Por padrão, esta coluna fica oculta.

- **% de 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 arquivos.

- **Limite rígido de arquivos**

  Exibe o limite rígido para o número de arquivos permitidos na cota. O valor é exibido como “Ilimitado” se a cota estiver definida sem um limite rígido de arquivos.

- **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 estiver definida sem um limite flexível de arquivos. Por padrão, esta coluna fica oculta.

- **Endereço de email**

  Exibe o endereço de e-mail do usuário ou do grupo de usuários para o qual são enviadas notificações quando ocorre uma violação das cotas.

Aba de compartilhamentos NFS

A aba Compartilhamentos NFS exibe informações sobre os compartilhamentos NFS, como seu status, o caminho associado ao volume (volumes FlexGroup ou volumes FlexVol), os níveis de acesso dos clientes aos compartilhamentos NFS e a política de exportação definida para os volumes que são 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 incluírem 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 de exportação NFS explícita 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 um qtree no volume, a coluna exibirá os nomes do volume e do qtree.

  Você pode clicar no link para ver detalhes sobre o objeto na respectiva página de detalhes. Se o objeto for uma qtree, os links são exibidos tanto para a qtree quanto para o volume.

- **Estado do volume**

  Exibe o estado do volume que está sendo exportado. O estado pode ser Offline, Online, Restrito ou Misto.

  - Offline

    Não é permitido o acesso de leitura ou gravação ao volume.

  - Online

    O acesso de leitura e gravação ao volume é permitido.

  - Restrito

    Operações limitadas, como reconstrução de paridade, são permitidas, mas o acesso aos dados não é permitido.

  - Misto

Os componentes de um volume FlexGroup não estão todos no mesmo estado.

- **estilo de segurança**

  Exibe as permissões de acesso para os volumes exportados. O estilo de segurança pode ser UNIX, Unified, NTFS ou Mixed.

  - UNIX (clientes NFS)

    Os arquivos e diretórios no volume possuem permissões UNIX.

  - Unificado

    Os arquivos e diretórios no volume possuem um estilo de segurança unificado.

  - NTFS (clientes CIFS)

    Os arquivos e diretórios no volume possuem permissões NTFS do Windows.

  - Misto

    Os arquivos e diretórios no volume podem ter permissões UNIX ou permissões NTFS do Windows.

- **Permissão UNIX**

  Exibe os bits de permissão UNIX em formato de string octal, definidos para os volumes exportados. É semelhante aos bits de permissão no estilo UNIX.

- **Política de exportação**

  Exibe as regras que definem a permissão de acesso para os volumes exportados. Você pode clicar no link para visualizar detalhes sobre as regras associadas à política de exportação, como os protocolos de autenticação e a permissão de acesso.

Guia Compartilhamentos SMB

Exibe informações sobre os compartilhamentos SMB na VM de 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.

Os compartilhamentos em pastas não são exibidos na guia SMB Shares.

- **Botão de comando View User Mapping**

  Abre a caixa de diálogo Mapeamento de Usuário.

  Você pode visualizar os detalhes do mapeamento de usuários para a máquina virtual de armazenamento.

- **Mostrar botão de comando ACL**

  Abre a caixa de diálogo de Controle de Acesso para o compartilhamento.

Você pode visualizar os 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 foi criado.

- **Caminho de Junção Ativo**

  Exibe se o caminho para acessar o compartilhamento está ativo ou inativo.

- **Objeto que contém**

  Exibe o nome do objeto que contém o compartilhamento. O objeto que contém o compartilhamento pode ser um volume ou uma qtree.

  Ao clicar no link, você pode visualizar detalhes sobre o objeto contêiner na respectiva página Details. Se o objeto contêiner for um qtree, serão exibidos links para o qtree e para o volume.

- **Estado do volume**

  Exibe o estado do volume que está sendo exportado. O estado pode ser Offline, Online, Restrito ou Misto.

  - Offline

    Não é permitido o acesso de leitura ou gravação ao volume.

  - Online

    O acesso de leitura e gravação ao volume é permitido.

  - Restrito

    Operações limitadas, como reconstrução de paridade, são permitidas, mas o acesso aos dados não é permitido.

  - Misto

    Os componentes de um volume FlexGroup não estão todos no mesmo estado.

- **Segurança**

  Exibe as permissões de acesso para os volumes exportados. O estilo de segurança pode ser UNIX, Unified, NTFS ou Mixed.

  - UNIX (clientes NFS)

    Os arquivos e diretórios no volume possuem permissões UNIX.

- Unificado

  Os arquivos e diretórios no volume possuem um estilo de segurança unificado.

- NTFS (clientes CIFS)

  Os arquivos e diretórios no volume possuem permissões NTFS do Windows.

- Misto

  Os arquivos e diretórios no volume podem ter permissões UNIX ou permissões NTFS do Windows.

- **Política de exportação**

  Exibe o nome da política de exportação aplicável ao compartilhamento. Se nenhuma política de exportação for especificada para a máquina virtual de armazenamento, o valor será exibido como "Não ativado".

  Você pode clicar no link para visualizar detalhes sobre as regras associadas à política de exportação, como protocolos de acesso e permissões. O link fica desabilitado se a política de exportação estiver desabilitada para a máquina virtual de armazenamento selecionada.

- **Equivalente NFS**

  Especifica se existe um equivalente NFS para o compartilhamento.

Guia SAN

Exibe detalhes sobre LUNs, grupos de iniciadores e iniciadores para a VM de armazenamento selecionada. Por padrão, a visualização de LUNs é exibida. Você pode visualizar detalhes sobre os grupos de iniciadores na guia Grupos de Iniciadores e detalhes sobre os iniciadores na guia Iniciadores.

- **Aba LUNs**

  Exibe detalhes sobre as LUNs pertencentes à VM de armazenamento selecionada. Você pode visualizar informações como o nome da LUN, o estado da LUN (online ou offline), o nome do sistema de arquivos (volume ou qtree) que contém a LUN, o tipo de sistema operacional do host, a capacidade total de dados e o número de série da LUN. A coluna Desempenho da LUN fornece um link para a página de detalhes de LUN/Performance.

  Você também pode visualizar informações para saber se thin provisioning 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.

- **Aba Grupos de Iniciadores**

  Exibe detalhes sobre grupos de iniciadores. Você pode visualizar detalhes como o nome do grupo de iniciadores, o estado de acesso, o tipo de sistema operacional usado por todos os iniciadores do grupo e o protocolo compatível. Ao clicar no link na coluna de estado de acesso, você pode visualizar o estado de acesso atual do grupo de iniciadores.

  - **Normal**

    O grupo iniciador está conectado a múltiplos caminhos de acesso.

- **Caminho Único**

  O grupo de iniciadores está conectado a um único caminho de acesso.

- **Sem Caminhos**

  Não há nenhum caminho de acesso conectado ao grupo de iniciadores.

  Você pode visualizar se os grupos de iniciadores estão mapeados para todas as interfaces ou para interfaces específicas por meio de um conjunto de portas. Ao clicar no link de contagem na coluna Interfaces mapeadas, todas as interfaces são exibidas ou apenas as interfaces específicas de um conjunto de portas. As 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.

- **Aba Iniciadores**

  Exibe o nome e o tipo do iniciador e o número total de grupos de iniciadores mapeados para esse iniciador na máquina virtual 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 storage selecionada. Os detalhes incluem o nome da anotação e os valores de anotação aplicados à VM de storage. Você também pode remover anotações manuais do painel Anotações Relacionadas.

Painel de dispositivos relacionados

O painel Dispositivos Relacionados permite visualizar o cluster, os agregados e os volumes relacionados à VM de armazenamento:

- **Cluster**

  Exibe o estado de integridade do cluster ao qual a máquina virtual de armazenamento pertence.

- **Agregados**

  Exibe o número de agregados que pertencem à VM de armazenamento selecionada. O status de integridade dos agregados também é exibido, com base no nível de gravidade mais alto. Por exemplo, se uma VM de armazenamento contiver dez agregados, cinco dos quais exibem o status de Aviso e os cinco restantes exibem o status Crítico, o status exibido será Crítico.

- **Agregados Atribuídos**

  Exibe o número de agregados atribuídos a uma máquina virtual de storage. O status de integridade 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 severidade mais alto. Quando

há volumes FlexGroup na VM de armazenamento, a contagem também inclui FlexGroups; ela não inclui os constituintes do FlexGroup.

Painel de Grupos Relacionados

O painel Grupos Relacionados permite que você visualize a lista de grupos associados à VM de storage selecionada.

Painel de alertas relacionados

O painel Alertas Relacionados permite visualizar 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.

Visualize a página de detalhes do cluster/saúde em Active IQ Unified Manager

A página de detalhes Cluster / Health 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; ou seja, se o Unified Manager consegue 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 navegar até a página Cluster / Performance details.

- **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, permitindo que o Unified Manager detecte alterações recentes no cluster.

    Se o Unified Manager estiver emparelhado com o OnCommand Workflow Automation, a operação de redescoberta também recuperará os dados em cache do WFA, se houver.

  Após o início da operação de redescoberta, um link para os detalhes da tarefa associada é exibido para permitir o acompanhamento do status da tarefa.

  - Anotar: permite adicionar anotações ao cluster selecionado.

- **Visualizar Clusters**

  Permite que você navegue até a visualização Saúde: todos os clusters.

Aba Saúde

Exibe informações detalhadas sobre os problemas de disponibilidade de dados e de capacidade de dados de vários objetos do cluster, como nós, SVMs e agregados. Os problemas de disponibilidade estão relacionados à capacidade dos objetos do cluster de fornecer dados. Os problemas de capacidade estão relacionados à capacidade dos objetos do cluster de armazenar dados.

Você pode clicar no gráfico de um objeto para visualizar uma lista filtrada dos objetos. Por exemplo, você pode clicar no gráfico de capacidade de SVM que exibe avisos para visualizar uma lista filtrada de SVMs. Essa lista contém SVMs que possuem volumes ou qtrees com problemas de capacidade classificados como "Warning". Você também pode clicar no gráfico de disponibilidade de SVMs que exibe avisos para visualizar a lista de SVMs com problemas de disponibilidade classificados como "Warning".

Problemas de disponibilidade

Exibe graficamente o número total de objetos, incluindo aqueles com problemas de disponibilidade e aqueles sem problemas relacionados à disponibilidade. As cores no gráfico representam os diferentes níveis de gravidade dos problemas. As informações abaixo do gráfico fornecem detalhes sobre os problemas de disponibilidade que podem afetar ou já afetaram a disponibilidade dos dados no cluster. Por exemplo, exibe informações sobre gavetas de disco inativas e agregados offline.

Os dados exibidos no gráfico de barras do SFO são baseados no estado de alta disponibilidade (HA) dos nós. Os dados exibidos em todos os outros gráficos de barras são calculados com base nos eventos gerados.

Problemas de capacidade

Exibe graficamente o número total de objetos, incluindo aqueles com problemas de capacidade e aqueles sem problemas relacionados à capacidade. As cores no gráfico representam os diferentes níveis de gravidade dos problemas. As informações abaixo do gráfico fornecem detalhes sobre problemas de capacidade que podem afetar ou já afetaram a capacidade de dados no cluster. Por exemplo, são exibidas informações sobre agregados que provavelmente ultrapassarão os valores de limite definidos.

Aba Capacidade

Exibe informações detalhadas sobre a capacidade do cluster selecionado.

Capacidade

Exibe o gráfico de capacidade de dados mostrando a capacidade utilizada e a capacidade disponível de todos os agregados alocados:

- Espaço lógico utilizado

  O tamanho real dos dados armazenados em todos os agregados deste cluster, sem aplicar a economia do uso das tecnologias de eficiência de storage do ONTAP. Isso não inclui cópias Snapshot.

- Redução de dados

  Exibe a proporção sem cópias Snapshot e com dois dígitos significativos, por exemplo, 1,8 para 1. Essa proporção se baseia nas configurações de eficiência de storage do ONTAP.

- Usado

  A capacidade física utilizada pelos dados em todos os agregados. Isso não inclui a capacidade utilizada

para paridade, dimensionar corretamente e reserva.

- Disponível

  Exibe a capacidade disponível para dados.

- Peças de reposição

  Exibe a capacidade de armazenamento disponível em 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 do agregado de raiz.

- Capacidade total

  Exibe a capacidade total do cluster. Isso não inclui a capacidade atribuída à paridade.

- Usado

  Exibe a capacidade utilizada pelos dados. Isso não inclui a capacidade utilizada para paridade, dimensionar corretamente 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 em todos os discos sobressalentes.

Nível de nuvem

Exibe a capacidade total da camada de nuvem usada e a capacidade usada para cada camada de nuvem conectada para os agregados habilitados para FabricPool no cluster. O FabricPool pode ser licenciado ou não licenciado.

Detalhamento da capacidade física por tipo de disco

A seção "Detalhes da capacidade física por tipo de disco" exibe informações detalhadas sobre a capacidade dos vários tipos de discos no cluster. Ao clicar no tipo de disco, você pode visualizar mais informações sobre ele na guia "Discos".

- Capacidade total utilizável

  Exibe a capacidade disponível e a capacidade ociosa 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 sobressalente dos discos de dados no HDD.

- Flash
  - SSD Data

    Exibe graficamente a capacidade utilizada e a capacidade disponível dos discos SSD de dados no cluster.

  - Cache SSD

    Exibe graficamente a capacidade de armazenamento dos discos de cache SSD no cluster.

  - SSD sobressalente

    Exibe graficamente a capacidade disponível 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 relacionados à capacidade.

- Status

  Indica que o agregado apresenta 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 data e a hora em que o evento foi acionado, o nome do administrador ao qual o evento está atribuído e a causa do evento. Você pode clicar no botão **Ver detalhes** para visualizar mais informações sobre o evento.

  Se o status do agregado for determinado por vários eventos da mesma gravidade, os três principais eventos serão exibidos com informações como o nome do evento, a hora e a data em que os eventos são acionados e o nome do administrador ao qual o evento está atribuído. Você pode visualizar mais detalhes sobre cada um desses eventos clicando no nome do evento. Você também pode clicar no link **View All Events** para visualizar a lista de eventos gerados.

  > Um agregado pode ter vários eventos relacionados à capacidade com a mesma gravidade ou com gravidades diferentes. No entanto, apenas a gravidade mais alta é exibida. Por exemplo, se um agregado tiver dois eventos com níveis de gravidade "Erro" e "Crítico", apenas a gravidade "Crítico" é exibida.

- Agregado

  Exibe o nome do agregado.

- Capacidade de dados utilizada

  Exibe graficamente informações sobre a utilização da capacidade do agregado (em porcentagem).

- Dias até encher

  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 a LIF de gerenciamento de cluster que o Unified Manager usa para se conectar ao cluster. Também exibe o status operacional da interface.

- Nome do host ou endereço IP

  Exibe o FQDN, o nome abreviado ou o endereço IP da LIF de gerenciamento de cluster que o Unified Manager usa para se conectar ao cluster.

- FQDN

  Exibe o nome de domínio totalmente qualificado (FQDN) do cluster.

- Versão do OS

  Exibe a versão do ONTAP que o cluster está executando. Se os nós do 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.

- Cluster

  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, o nome abreviado ou o endereço IP do cluster remoto.

- Localização

  Exibe a localização do cluster remoto.

MetroCluster Visão geral

Fornece detalhes sobre o cluster local em configurações de MetroCluster over FC ou MetroCluster over IP. Essas informações são exibidas apenas para configurações de MetroCluster over FC ou IP.

- Tipo

  Exibe se o tipo do MetroCluster é de dois nós ou de quatro nós. Para o MetroCluster via IP, há suporte apenas para quatro nós.

- Configuração

  Exibe a configuração do MetroCluster em FC e IP, que pode ter os seguintes valores:

Para FC

- Configuração estendida com cabos SAS
- Configuração estendida com ponte FC-SAS
- Configuração de malha com switches FC

> Para uma configuração do MetroCluster de quatro nós, somente a configuração de malha com switches FC é compatível.

Para IP

- Configuração de IP com switches Ethernet (L2 ou L3, dependendo de como o cluster está configurado)
  - Switchover automático não planejado (AUSO)

    Exibe se o switchover não planejado automatizado (AUSO) está habilitado para o cluster local. Por padrão, a AUSO está habilitada para todos os clusters em uma configuração de dois nós do MetroCluster no Unified Manager. Você pode usar a interface de linha de comando para alterar a configuração da AUSO. Isso é compatível apenas com o MetroCluster over FC.

  - Modo de switchover

    Exibe o modo de switchover para a configuração do MetroCluster over IP. Os valores disponíveis são: `Active`, `Negotiated Switchover`, e `Automatic Unplanned Switchover`.

Nós

- Disponibilidade

  Exibe o número de nós que estão ativos ( ) ou inativos ( ) no cluster.

- Versões do SO

Exibe as versões do ONTAP que os nós estão executando, bem como o número de nós que executam uma versão específica do ONTAP. Por exemplo, 9.6 (2), 9.3 (1) especifica que dois nós estão executando o ONTAP 9.6 e um nó está executando o ONTAP 9.3.

Máquinas Virtuais de Armazenamento

- Disponibilidade

  Exibe o número de SVMs que estão ativas ( ) ou inativas ( ) no cluster.

Interfaces de rede

- Disponibilidade

  Exibe o número de LIFs que não são de dados e estão ativas ( ) ou inativas ( ) no cluster.

- Interfaces de gerenciamento de clusters

  Exibe o número de LIFs de gerenciamento de cluster.

- Interfaces de gerenciamento de nós

  Exibe o número de LIFs de gerenciamento de nós.

- Interfaces de cluster

  Exibe o número de LIFs do cluster.

- Interfaces entre clusters

  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 oferece suporte a mediadores e o status de conectividade do mediador. Indica se o mediador está configurado e, em caso afirmativo, exibe o status dos mediadores.

  - Não aplicável

    Exibe uma mensagem quando o cluster não oferece suporte a mediadores.

  - Não configurado

    Aparece quando o cluster oferece suporte a mediadores, mas o mediador não está configurado.

  - Endereço IP

Exibe quando o cluster suporta mediadores e quando o mediador está configurado. O status do mediador é indicado por cor. A cor verde indica que o mediador está acessível. A cor vermelha indica que o mediador está inacessível.

Tiers de nuvem

Lista os nomes das camadas de nuvem às quais este cluster está conectado. 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 Conectividade do MetroCluster

Exibe os problemas e o status de conectividade dos componentes do cluster na configuração do MetroCluster over FC. Um cluster é exibido em uma caixa vermelha quando o parceiro de recuperação de desastres do cluster apresenta problemas.

A guia Conectividade do MetroCluster é exibida apenas para clusters que estão em uma configuração MetroCluster over 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 aba do nó na página de detalhes do cluster. Clicar no link de contagem dos discos no cluster remoto exibe a aba de discos na página de detalhes do cluster remoto.

Ao gerenciar uma configuração de oito nós do MetroCluster, clicar no link de contagem do componente "Disk Shelves" exibe apenas as gavetas de disco locais do par de HA padrão. Além disso, não há como exibir as gavetas de disco locais no outro par de HA.

Você pode mover o ponteiro sobre os componentes para ver os detalhes e o status de conectividade dos clusters em caso de algum problema, bem como mais informações sobre o evento ou os eventos gerados para o problema.

Se o status do problema de conectividade entre os componentes for determinado por um único evento, você poderá visualizar informações como o nome do evento, a data e a hora em que o evento foi acionado, o nome do administrador ao qual o evento está atribuído e a causa do evento. O botão Exibir detalhes fornece mais informações sobre o evento.

Se o status do problema de conectividade entre os componentes for determinado por vários eventos da mesma gravidade, os três principais eventos serão exibidos com informações como o nome do evento, a hora e a data em que os eventos são acionados e o nome do administrador ao qual o evento está atribuído. Você pode visualizar 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.

MetroCluster aba de Replicação

Exibe o status dos dados que estão sendo replicados em uma configuração MetroCluster over FC. Você pode usar a guia MetroCluster Replication para garantir a proteção de dados espelhando os dados de forma síncrona com os clusters já emparelhados. Um cluster é exibido em uma caixa vermelha quando o parceiro de recuperação de desastres do cluster apresenta problemas.

A aba Replicação do MetroCluster é exibida apenas para clusters que estão em uma configuração de MetroCluster over FC.

Em um ambiente do MetroCluster, você pode usar esta guia para verificar as conexões lógicas e o emparelhamento 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 problemas que podem ocorrer durante o espelhamento de metadados e dados.

Na guia MetroCluster Replication, 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 todas as LIFs não relacionadas a dados que foram criadas no cluster selecionado.

Interface de rede

Exibe o nome da LIF criada no cluster selecionado.

Status operacional

Exibe o status operacional da interface, que pode ser Up (), Down () ou Unknown (). O status operacional de uma interface de rede é determinado pelo status de suas portas físicas.

Status administrativo

Exibe o status administrativo da interface, que pode ser Up (), Down () ou Unknown (). 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. No entanto, se o status administrativo de uma LIF for Down, o status operacional será Down 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.

Porta inicial

Exibe a porta física à qual a interface estava originalmente associada.

Porta atual

Exibe a porta física à qual a interface está atualmente associada. Após a migração de LIF, a porta atual pode ser diferente da porta inicial.

Política de failover

Exibe a política de failover configurada para a interface.

Grupos de roteamento

Exibe o nome do grupo de roteamento. Você pode visualizar mais informações sobre as rotas e o gateway de destino clicando no nome do grupo de roteamento.

Os grupos de roteamento não são compatíveis com o ONTAP 8.3 ou posterior e, portanto, é exibida uma coluna em branco para esses clusters.

Grupo de failover

Exibe o nome do grupo de failover.

Aba Nodes

Exibe informações sobre os nós no cluster selecionado. Você pode visualizar informações detalhadas sobre os pares de HA, gavetas de discos e portas:

Detalhes de HA

Fornece uma representação pictórica do estado de HA e do estado de saúde dos nós no par de HA. O estado de saúde do nó é indicado pelas seguintes cores:

- **Verde**

  O nó está em funcionamento.

- **Amarelo**

  O nó assumiu o controle do nó parceiro ou está enfrentando problemas ambientais.

- **Vermelho**

  O nó está inativo.

Você pode visualizar informações sobre a disponibilidade do par de HA e tomar as medidas necessárias para evitar quaisquer riscos. Por exemplo, no caso de uma possível operação de takeover, a seguinte mensagem é exibida: Storage failover possible.

Você pode visualizar uma lista dos eventos relacionados ao par de HA e ao seu ambiente, como ventoinhas, fontes de alimentação, bateria NVRAM, cartões flash, processador de serviço e conectividade dos gabinetes de disco. Você também pode visualizar a hora em que os eventos foram acionados.

Você pode visualizar outras informações relacionadas ao nó, como o número do modelo.

Caso existam clusters de nó único, você também poderá visualizar detalhes sobre os nós.

Gavetas de disco

Exibe informações sobre as gavetas de disco no par de HA.

Você também pode visualizar os eventos gerados para os gabinetes de discos e os componentes ambientais, bem como o horário em que os eventos foram acionados.

- **ID do shelf**

  Exibe o ID da gaveta onde o disco está localizado.

- **Status do componente**

  Exibe detalhes ambientais das gavetas de discos, como fontes de alimentação, ventoinhas, sensores de

temperatura, sensores de corrente, conectividade dos discos e sensores de tensão. 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 dos componentes ambientais estão inativos.

- **Estado**

  Exibe o estado da gaveta de discos. Os estados possíveis são Offline, Online, Sem status, Inicialização necessária, Ausente e Desconhecido.

- **Modelo**

  Exibe o número do modelo da gaveta de discos.

- **Prateleira de Discos Local**

  Indica se o compartimento de discos está localizado no cluster local ou no cluster remoto. Esta coluna é exibida apenas para clusters em uma configuração MetroCluster.

- **ID único**

  Exibe o identificador único da gaveta de discos.

- **Versão do firmware**

  Exibe a versão do firmware da gaveta de discos.

Portas

Exibe informações sobre as portas FC, FCoE e Ethernet associadas. Você pode visualizar detalhes sobre as portas e as LIFs associadas clicando nos ícones das portas.

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 World Wide Port Name (WWPN) da porta.

- Revisão do firmware

  Exibe a revisão de 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 à porta na lista de eventos. Você também pode visualizar os detalhes da LIF associada, como nome da LIF, status operacional, endereço IP ou WWPN, protocolos, nome da SVM associada à LIF, porta atual, política de failover e grupo de failover.

Guia Discos

Exibe detalhes sobre os discos no cluster selecionado. Você pode visualizar informações relacionadas aos discos, como o número de discos em uso, discos sobressalentes, discos com defeito 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 com falha, discos não atribuídos e discos não suportados. Se você clicar no link de contagem do tipo efetivo de disco, serão exibidos os discos do estado e do tipo efetivo selecionados. Por exemplo, se você clicar no link de contagem para o estado de disco "Broken" e o tipo efetivo SAS, serão exibidos todos os discos com o estado de disco "Broken" e o tipo efetivo SAS.

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, Reserva, Quebrado, Não atribuído, Não suportado ou Desconhecido. Por padrão, esta coluna é ordenada para exibir os estados na seguinte ordem: Quebrado, Não atribuído, Não suportado, Reserva, 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 apenas para clusters em uma configuração do 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 ao disco com falha. Você pode mover o cursor sobre o link de contagem para visualizar os agregados afetados e, em seguida, clicar no nome do agregado para ver os detalhes do agregado. Você também pode clicar na contagem de agregados para visualizar a lista de agregados afetados na visualização "Health: All Aggregates".

Nenhum valor é exibido nesta coluna nos seguintes casos:

- Para discos com defeito quando um cluster que contém esses discos é adicionado ao Unified Manager
- Quando não houver discos com falha

Pool de storage

Exibe o nome do pool de storage ao qual o SSD pertence. Você pode mover o ponteiro sobre o nome do pool de storage para visualizar os detalhes do pool de storage.

Capacidade armazenável

Exibe a capacidade de disco disponível para uso.

Capacidade bruta

Exibe a capacidade do disco bruto, não formatado, antes de dimensionar corretamente e configurar o RAID. Por padrão, esta coluna fica oculta.

Tipo

Exibe os tipos de discos: por exemplo, ATA, SATA, FCAL ou VMDISK.

Tipo efetivo

Exibe o tipo de disco atribuído pelo ONTAP.

Determinados tipos de disco do ONTAP são considerados equivalentes para fins de criação e adição a agregados, bem como para o gerenciamento de discos sobressalentes. O ONTAP atribui um tipo de disco efetivo a cada tipo de disco.

Blocos sobressalentes consumidos %

Exibe, em porcentagem, os blocos sobressalentes que estão sendo consumidos no disco SSD. Esta coluna fica em branco para discos que não sejam SSD.

% de vida útil usada

Exibe, em porcentagem, uma estimativa da vida útil do SSD usada, com base no uso real do SSD e na previsão da vida útil do SSD pelo fabricante. Um valor superior a 99 indica que a resistência estimada foi consumida, mas isso não significa necessariamente falha do SSD. Se o valor for desconhecido, o disco será omitido.

Firmware

Exibe a versão do firmware do disco.

RPM

Exibe as rotações 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 do compartimento

Exibe o ID da gaveta onde o disco está localizado.

Baía

Exibe o ID do compartimento onde o disco está.

Painel de anotações relacionadas

Permite visualizar os detalhes das anotações associadas ao cluster selecionado. Os detalhes incluem o nome da anotação e os valores de anotação aplicados ao cluster. Você também pode remover anotações manuais no painel "Related Annotations".

Painel de dispositivos relacionados

Permite visualizar os detalhes dos dispositivos associados ao cluster selecionado.

Os detalhes incluem propriedades do dispositivo conectado ao cluster, como o tipo de dispositivo, o tamanho, a quantidade e o estado de integridade. Você pode clicar no link da quantidade para fazer uma análise mais detalhada desse dispositivo específico.

Você pode usar o painel Parceiro do MetroCluster para obter a 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 apenas para clusters em uma configuração do MetroCluster.

O painel Dispositivos Relacionados permite visualizar e navegar até os nós, SVMs e agregados relacionados ao cluster:

MetroCluster Parceiro

Exibe o estado de saúde do parceiro do MetroCluster. Usando o link de contagem, você pode navegar mais a fundo e obter informações sobre a saúde 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. A capacidade indica a capacidade utilizável total em relação à capacidade disponível.

Máquinas Virtuais de Armazenamento

Exibe o número de SVMs que pertencem ao cluster selecionado.

Agregados

Exibe o número, a capacidade e o estado de saúde dos agregados que pertencem ao cluster selecionado.

Painel de Grupos Relacionados

Permite visualizar a lista de grupos que inclui o cluster selecionado.

Painel de alertas relacionados

O painel Alertas Relacionados permite visualizar a lista de alertas para o cluster selecionado. Você também pode adicionar um alerta clicando no link Adicionar Alerta ou editar um alerta existente clicando no nome do alerta.

Informações relacionadas

"Página de volumes" "Visualizando a lista e os detalhes dos clusters"

Visualize a página de detalhes de agregado/de saúde no Active IQ Unified Manager

Você pode usar a página Detalhes de agregado/Saúde para visualizar informações detalhadas sobre o agregado selecionado, como capacidade, informações de disco, detalhes de configuração e eventos gerados. Você também pode visualizar informações sobre os objetos relacionados e os alertas relacionados a esse agregado.

Botões de comando

> Ao monitorar um agregado habilitado para o FabricPool, os valores comprometidos e sobrecomprometidos nesta página são relevantes apenas para a capacidade local, ou da camada de desempenho. A quantidade de espaço disponível na camada de nuvem não se reflete nos valores sobrecomprometidos. Da mesma forma, os valores de limite do agregado são relevantes apenas para a camada 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 navegar até a página de detalhes de agregado / desempenho.

- **Ações**
  - Adicionar alerta

    Permite que você adicione um alerta ao agregado selecionado.

  - Editar limites

    Permite modificar as configurações de limite para o agregado selecionado.

- **Ver agregados**

  Permite navegar até a visualização Saúde: todos os agregados.

Aba Capacidade

A aba Capacidade exibe informações detalhadas sobre o agregado selecionado, como sua capacidade, limites e taxa de crescimento diário.

Por padrão, eventos de capacidade não são gerados para agregados de raiz. Além disso, os valores de limite usados pelo Unified Manager não se aplicam a agregados de raiz do nó. Somente um representante do suporte técnico pode modificar as configurações para que esses eventos sejam gerados. Quando um representante do suporte técnico modifica as configurações, os valores de limite são aplicados ao agregado de raiz do nó.

- **Capacidade**

  Exibe o gráfico de capacidade de dados e o gráfico de cópias Snapshot, que mostram detalhes da capacidade do agregado:

  - Espaço lógico utilizado

    O tamanho real dos dados armazenados no agregado, sem aplicar as economias obtidas com o uso das tecnologias de eficiência de storage do ONTAP.

  - Usado

    A capacidade física usada pelos dados no agregado.

  - Supercomprometido

    Quando o espaço no agregado está superalocado, o gráfico exibe um indicador com a quantidade superalocada.

  - Aviso

    Exibe uma linha pontilhada no local em que o limite de aviso está definido; isso significa que o espaço no agregado está quase cheio. Se esse limite for ultrapassado, o evento "Space Nearly Full" será gerado.

  - Erro

    Exibe uma linha contínua no local em que o limite de erro está definido; isso significa que o espaço no agregado está cheio. Se esse limite for ultrapassado, o evento Space Full será gerado.

  - Gráfico de cópias Snapshot

Este gráfico é exibido somente quando a capacidade de Snapshot utilizada ou a reserva do Snapshot não for zero.

Ambos os gráficos exibem a capacidade pela qual a capacidade de Snapshot excede a reserva do Snapshot se a capacidade de Snapshot usada exceder a reserva do Snapshot.

- **Nível de nuvem**

  Exibe o espaço usado pelos dados na camada de nuvem para agregados habilitados para o FabricPool. O FabricPool pode ser licenciado ou não licenciado.

  Quando a camada de nuvem é espelhada em outro provedor de nuvem (a “camada de espelho”), ambas as camadas de nuvem são exibidas aqui.

- **Detalhes**

  Exibe informações detalhadas sobre a capacidade.

  - Capacidade total

    Exibe a capacidade total no agregado.

  - Capacidade de dados

    Exibe a quantidade de espaço utilizado pelo agregado (capacidade utilizada) e a quantidade de espaço disponível no agregado (capacidade livre).

  - Reserva do Snapshot

    Exibe a capacidade de Snapshot usada e livre do agregado.

  - Capacidade com comprometimento em excesso

    Exibe o comprometimento em excesso do agregado. O comprometimento em excesso do agregado permite fornecer mais armazenamento do que o realmente disponível em um determinado agregado, desde que nem todo esse armazenamento esteja sendo usado no momento. Quando o thin provisioning está em uso, o tamanho total dos volumes no agregado pode exceder a capacidade total do agregado.

    Se você tiver comprometimento em excesso no seu agregado, deverá monitorar cuidadosamente o espaço disponível e adicionar armazenamento conforme necessário para evitar erros de gravação por falta de espaço.

  - Nível de nuvem

    Exibe o espaço usado pelos dados na camada de nuvem para agregados habilitados para FabricPool. O FabricPool pode ser licenciado ou não licenciado. Quando a camada de nuvem é espelhada em outro provedor de nuvem (a camada espelho), ambas as camadas de nuvem são exibidas aqui.

  - Espaço total do cache

    Exibe o espaço total das unidades de estado sólido (SSDs) ou unidades de alocação adicionadas a um agregado do Flash Pool. Se você habilitou o Flash Pool para um agregado, mas não adicionou nenhum SSD, o espaço de cache será exibido como 0 KB.

Este campo fica oculto se o Flash Pool estiver desativado para um agregado.

- Limiares de agregados

  Exibe os seguintes limites de capacidade do agregado:

  - Limiar de quase cheio

    Especifica a porcentagem em que um agregado está quase cheio.

  - Limiar total

    Especifica a porcentagem em que um agregado está cheio.

  - Limiar de comprometimento em excesso quase atingido

    Especifica a porcentagem na qual um agregado está quase com comprometimento em excesso.

  - Limiar de comprometimento em excesso

    Especifica a porcentagem na qual um agregado tem comprometimento em excesso.

- Outros detalhes: taxa de crescimento diário

  Exibe o espaço de disco usado no agregado se a taxa de alteração entre as duas últimas amostras continuar por 24 horas.

  Por exemplo, se um agregado utiliza 10 GB de espaço de disco às 14:00 e 12 GB às 18:00, a taxa de crescimento diário (GB) para esse agregado é de 2 GB.

- Movimentação de volume

  Exibe o número de operações de movimentação de volume que estão em andamento:

  - Volumes de saída

    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 é movido, o status da operação de movimentação do volume e a hora prevista de término.

  - Volumes em

    Exibe o número e a capacidade restante dos volumes que estão sendo movidos para o agregado.

Você pode clicar no link para visualizar mais detalhes, como o nome do volume, o agregado de onde o volume é movido, o status da operação de movimentação do volume e a hora prevista de término.

- Capacidade utilizada estimada após a movimentação de volume

  Exibe a quantidade estimada de espaço utilizado, em porcentagem e em KB, MB, GB etc., 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 utilizada pelo volume (capacidade utilizada) e a quantidade de espaço disponível (capacidade livre) no volume são exibidas. Quando o evento "Thin-Provisioned Volume Space At Risk" é gerado para volumes com thin provisioning, a quantidade de espaço utilizada pelo volume (capacidade utilizada) e a quantidade de espaço disponível no volume, mas que não pode ser utilizada (capacidade inutilizável) devido a problemas de capacidade do agregado, são exibidas.

Você pode selecionar o gráfico que deseja visualizar nas listas suspensas. Você pode classificar os dados exibidos no gráfico para mostrar 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 thin provisioning. 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 de 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 a baia, a prateleira e a velocidade de rotação do disco, posicionando o cursor sobre os discos de paridade e os discos de dados.

- **Dados**

  Exibe graficamente detalhes sobre discos de dados dedicados, discos de dados compartilhados ou ambos. Quando os discos de dados contêm discos compartilhados, os detalhes gráficos dos discos compartilhados são exibidos. Quando os discos de dados contêm discos dedicados e discos compartilhados, os detalhes gráficos dos discos de dados dedicados e dos discos de dados compartilhados são exibidos.

  - **Detalhes do RAID**

    Os detalhes do RAID são exibidos apenas para discos dedicados.

    - Tipo

      Exibe o tipo 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 Utilizados**
    - Tipo efetivo

      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 dos

discos 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 dos discos 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 dos discos compartilhados são exibidos somente quando o agregado contém discos compartilhados.

◦ **Discos sobressalentes**

Exibe o tipo efetivo, o número e a capacidade dos discos de dados sobressalentes 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**

Fornece detalhes sobre discos SSD de cache dedicados e discos SSD de cache compartilhados.

Os seguintes detalhes dos discos SSD de cache dedicados 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 Utilizados**

- Tipo efetivo

  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 de disco, o número e a capacidade dos discos sobressalentes 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 storage**

Exibe o nome do pool de storage. Você pode mover o ponteiro sobre o nome do pool de storage para visualizar os seguintes detalhes:

- Status

  Exibe o status do pool de storage, que pode estar íntegro ou não íntegro.

- Alocações totais

  Exibe o total de unidades de alocação e o tamanho no pool de storage.

- Tamanho da unidade de alocação

  Exibe a quantidade mínima de espaço no pool de storage que pode ser alocada a um agregado.

- Discos

  Exibe o número de discos usados para criar o pool de storage. Se a contagem de discos na coluna do pool de storage e o número de discos exibido na guia Informações do Disco para esse pool de storage não coincidirem, isso indica que um ou mais discos estão com defeito e que o pool de storage não está íntegro.

- Alocação utilizada

  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 do agregado.

◦ **Cache alocado**

Exibe o tamanho das unidades de alocação usadas pelo agregado.

◦ **Unidades de Alocação**

Exibe o número de unidades de alocação usadas pelo agregado.

◦ **Discos**

Exibe o número de discos contidos no pool de storage.

- **Detalhes**
  - Pool de storage

    Exibe o número de pools de storage.

  - Tamanho total

    Exibe o tamanho total dos pools de storage.

- **Nível de nuvem**

  Exibe o nome da camada de nuvem, caso você tenha configurado um agregado habilitado para o FabricPool, e mostra o espaço total utilizado. 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 aba Configuração exibe detalhes sobre o agregado selecionado, como seu nó de cluster, tipo de bloco, tipo de RAID, tamanho de RAID e número de grupos RAID:

- **Visão geral**
  - Nó

    Exibe o nome do nó que contém o agregado selecionado.

  - Tipo de bloco

    Exibe o formato de bloco do agregado: 32 bits ou 64 bits.

  - Tipo RAID

    Exibe o tipo de RAID (RAID0, RAID4, RAID-DP, RAID-TEC ou RAID misto).

  - Tamanho do RAID

    Exibe o tamanho do grupo RAID.

  - Grupos RAID

    Exibe o número de grupos RAID no agregado.

  - SnapLock Tipo

    Exibe o tipo de 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 storage. Quando a camada de nuvem é espelhada para outro provedor de nuvem (a “mirror tier”), ambas as camadas de nuvem são exibidas aqui.

  - Fornecedor

    Exibe o nome do provedor de armazenamento, por exemplo, o StorageGRID, o Amazon S3, o IBM

Cloud Object Storage, o Microsoft Azure Cloud, o Google Cloud Storage ou o 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 utilizada para comunicação com o provedor de nuvem.

- Chave de acesso ou conta

  Exibe a chave de acesso ou a 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 histórico

A área Histórico exibe gráficos que fornecem informações sobre a capacidade do agregado selecionado. Além disso, você pode clicar no botão **Exportar** para criar um relatório em formato CSV para o gráfico que 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 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 agregado estiver constantemente ultrapassando o limite "Nearly Full", você pode tomar a ação apropriada.

Os gráficos de histórico exibem as seguintes informações:

- **Capacidade do agregado utilizada (%)**

  Exibe a capacidade utilizada no agregado e a tendência de como a capacidade do agregado é usada com base no histórico de uso, em 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 ver os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma determinada área. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda correspondente. Por exemplo, quando você clica na legenda "Capacidade Utilizada", a linha do gráfico de Capacidade Utilizada fica oculta.

- **Capacidade usada do agregado vs Capacidade total**

  Exibe a tendência de como a capacidade agregada é usada com base no histórico de uso, bem como a capacidade utilizada e a capacidade total, como gráficos de linhas, em bytes, kilobytes, megabytes e assim por diante, no eixo vertical (y). O período 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 determinada área. Você pode ocultar ou exibir um gráfico de linhas clicando na legenda apropriada. Por exemplo, ao clicar na legenda "Trend Capacity Used", a linha do gráfico Trend Capacity Used fica oculta.

- **Capacidade utilizada do agregado (%) vs capacidade comprometida (%)**

  Exibe a tendência de como a capacidade agregada é usada com base no histórico de uso, bem como o espaço comprometido, em gráficos de linha, em porcentagem, no eixo vertical (y). O período é exibido no eixo horizontal (x). Você pode selecionar um período de uma semana, um mês ou um ano. Você pode ver os detalhes de pontos específicos no gráfico posicionando o cursor sobre uma determinada área. Você pode ocultar ou exibir um gráfico de linha clicando na legenda correspondente. Por exemplo, ao clicar 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.

- **Hora de acionamento**

  Exibe o tempo decorrido desde que o evento foi gerado. Se o tempo decorrido for superior a uma semana, o registro de data e hora em que o evento foi gerado será exibido.

Painel de dispositivos relacionados

O painel Dispositivos Relacionados permite visualizar o nó de cluster, os volumes e os discos relacionados ao agregado:

- **Nó**

  Exibe a capacidade e o estado de saúde do nó que contém o agregado. A capacidade indica a capacidade utilizável total em relação à capacidade disponível.

- **Agregados no nó**

  Exibe o número e a capacidade de todos os agregados no nó de cluster que contém o agregado selecionado. O status de integridade dos agregados também é exibido, com base no nível de gravidade mais alto. Por exemplo, se um nó de cluster contiver dez agregados, cinco dos quais exibem o status de Aviso e os cinco restantes exibem o status Crítico, o status exibido será Crítico.

- **Volumes**

  Exibe o número e a capacidade dos volumes FlexVol e dos volumes FlexGroup no agregado; o número não inclui os constituintes do FlexGroup. O estado 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 visualizar 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 storage"

Proteger e restaurar dados

Criar e solucionar problemas em relacionamentos de proteção

Tipos de proteção do SnapMirror no Active IQ Unified Manager

Dependendo da implantação da sua topologia de storage, o Unified Manager permite que você configure vários tipos de relações de proteção do SnapMirror. Todas as variações da proteção do SnapMirror oferecem proteção de recuperação de desastres com failover, mas oferecem diferentes recursos em desempenho, flexibilidade de versão e proteção de várias cópias de backup.

Relacionamentos tradicionais de proteção assíncrona do SnapMirror

A proteção assíncrona tradicional do SnapMirror fornece proteção de espelhamento com replicação em bloco entre os volumes de origem e de destino.

Em relacionamentos tradicionais do SnapMirror, as operações de espelhamento são executadas mais rapidamente do que em relacionamentos alternativos do SnapMirror, porque a operação de espelhamento se baseia na replicação de blocos. No entanto, a proteção tradicional do SnapMirror exige que o volume de destino execute a mesma versão secundária ou uma versão secundária posterior do software ONTAP que o volume de origem, dentro da mesma versão principal (por exemplo, versão 8.x para 8.x ou 9.x para 9.x). Não há suporte para replicação de uma origem 9.1 para um destino 9.0, porque o destino está executando uma versão principal anterior.

SnapMirror Proteção assíncrona com replicação flexível entre versões

SnapMirror A proteção assíncrona com replicação flexível de versão fornece proteção de espelhamento de replicação lógica entre os volumes de origem e de destino, mesmo que esses volumes estejam sendo executados em versões diferentes do software ONTAP 8.3 ou posterior (por exemplo, da versão 8.3 para a 8.3.1, ou da 8.3 para a 9.1, ou da 9.2.2 para a 9.2).

Em relacionamentos do SnapMirror com replicação flexível em relação à versão, as operações de espelhamento não são executadas tão rapidamente quanto seriam em relacionamentos tradicionais do SnapMirror.

Devido à execução mais lenta, a proteção de replicação com flexibilidade de versão do SnapMirror não é adequada para implementação em nenhuma das seguintes circunstâncias:

- O objeto de origem contém mais de 10 milhões de arquivos a serem protegidos.
- O objetivo de 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 antigos do que duas horas em relação aos dados na origem.)

Em qualquer uma das circunstâncias listadas, é necessária a execução mais rápida da proteção padrão do SnapMirror baseada em replicação de blocos.

SnapMirror Proteção assíncrona com replicação flexível em relação à versão e opção de backup

O SnapMirror oferece proteção assíncrona com replicação flexível em relação à versão e opção de backup, fornecendo proteção de espelhamento entre os volumes de origem e de destino, além da capacidade de armazenar várias cópias dos dados espelhados no destino.

O administrador de storage pode especificar quais cópias Snapshot serão espelhadas da origem para o destino e também pode especificar por quanto tempo essas cópias devem ser mantidas no destino, mesmo que sejam excluídas na origem.

Em relacionamentos do SnapMirror com replicação flexível por versão e opção de backup, as operações de espelhamento não são executadas tão rapidamente quanto seriam em relacionamentos tradicionais do SnapMirror.

SnapMirror Replicação unificada (espelhamento 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 o SnapMirror, a proteção unificada de dados realiza uma transferência completa na primeira vez que você a invoca. Uma transferência completa sob a política padrão de proteção unificada de dados “MirrorAndVault” cria uma cópia Snapshot 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 unificada de dados não inclui cópias Snapshot mais antigas na transferência completa inicial.

SnapMirror Proteção síncrona com sincronização rigorosa

A proteção síncrona do SnapMirror com sincronização ""“strict”"" garante que os volumes primário e secundário sejam sempre cópias fiéis 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.

SnapMirror proteção síncrona com sincronização regular

SnapMirror A proteção síncrona com sincronização “regular” não exige que os volumes primário e secundário sejam sempre cópias exatas 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 dessincronizados, e a E/S do cliente continuará no volume primário.

> O botão Restaurar e os botões de operação de relacionamento não estão disponíveis ao monitorar relacionamentos de proteção síncrona na visualização Saúde: todos os volumes ou na página de detalhes de Volume/Saúde.

SnapMirror active sync

O recurso de sincronização ativa do SnapMirror está disponível com 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 e 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 storage do Unified Manager. SnapMirror active sync é compatível com clusters AFF ou clusters All SAN Array (ASA), em que os clusters primário e secundário podem ser AFF ou ASA. SnapMirror active sync protege aplicações com LUNs iSCSI ou FCP.

Ao visualizar os volumes e LUNs protegidos pela relação de sincronização ativa do SnapMirror, você pode obter uma visão unificada das relações de proteção, dos Grupos de Consistência no inventário de volumes,

visualizar a topologia de proteção das relações de Grupo de Consistência e visualizar dados históricos das relações de Grupo de Consistência por até um ano. Você também pode baixar o relatório. Você também pode visualizar o resumo das relações de Grupo de Consistência, pesquisar relações de Grupo de Consistência e obter informações sobre os volumes protegidos pelo Grupo de Consistência.

Na página Relacionamentos, você também pode classificar, filtrar e estender a proteção dos objetos de storage de origem e destino e de seu relacionamento que são protegidos pelo Consistency Group.

Para saber mais sobre o SnapMirror active sync, consulte "Documentação do ONTAP 9 para Snapmirror active sync (anteriormente SM-BC)".

Configure relações de proteção no Unified Manager

Configure relações de proteção no Active IQ Unified Manager

Existem várias etapas que você deve executar para usar o Unified Manager e o OnCommand Workflow Automation para configurar relações do SnapMirror e do SnapVault para proteger seus dados.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você deve ter estabelecido relacionamentos de peering entre dois clusters ou duas máquinas virtuais de armazenamento (SVMs).
- O OnCommand Workflow Automation deve ser integrado ao Unified Manager:
  - "Configure o OnCommand Workflow Automation".
  - "Verificando o armazenamento em cache da fonte de dados do Unified Manager no Workflow Automation".

Passos

1. Dependendo do tipo de relação de proteção que você deseja criar, faça um dos seguintes procedimentos:
   - "Criar uma relação de proteção do SnapMirror".
   - "Criar uma relação de proteção do SnapVault".
2. Se você deseja criar uma política para o relacionamento, dependendo do tipo de relacionamento que está criando, faça um dos seguintes procedimentos:
   - "Criar uma política do SnapVault".
   - "Criar uma política do SnapMirror".
3. "Crie um agendamento do SnapMirror ou do SnapVault".

Configure uma conexão entre o OnCommand Workflow Automation e o Active IQ 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, além de 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 gerenciamento de Clustered Data ONTAP" está incluído no WFA 5.1.1P6, portanto, não é necessário baixar este pacote da NetAppStorage Automation Store e instalá-lo separadamente em seu servidor WFA, como era necessário anteriormente. "Download WFA"

- Você precisa ter o nome do usuário do banco de dados que você criou no Unified Manager para dar suporte às conexões do WFA e do Unified Manager.

  Este usuário do banco de dados deve ter recebido a função de usuário Integration Schema.

- Você precisa ter a função de Administrador ou a função de Arquiteto atribuída no Workflow Automation.
- Você precisa ter o endereço do host, o número da porta 443, o nome de usuário e a senha para a configuração do Workflow Automation.
- Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **General** > **Workflow Automation**.
2. Na área **Usuário do Banco de Dados** da **página do Workflow Automation**, 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 do Workflow Automation.
3. Na área **Workflow Automation Credentials** da página, insira o nome do host ou o endereço IP (IPv4 ou IPv6), bem como o nome de usuário e a senha para a configuração do Workflow Automation.

   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 Workflow Automation é exibida.

6. Clique em **Sim** para recarregar a IU da web, e adicionar os recursos do Workflow Automation.

Informações relacionadas

"NetApp documentação: o OnCommand Workflow Automation (versões atuais)"

Verifique o Active IQ Unified Manager armazenamento em cache na Automação de Fluxo de Trabalho

Você pode determinar se o armazenamento em cache da fonte de dados do Unified Manager está funcionando corretamente verificando se a aquisição da fonte de dados foi bem-sucedida no Workflow Automation. Você pode fazer isso ao integrar o Workflow Automation com o Unified Manager para garantir que a funcionalidade do Workflow Automation esteja disponível após a integração.

Antes de começar

Para executar esta tarefa, você precisa ter a função Administrator ou a função Architect atribuída no Workflow Automation.

Passos

1. Na interface de usuário do Workflow Automation, selecione **Execução** > **Fontes de dados**.

2. Clique com o botão direito do mouse no nome da fonte de dados do Unified Manager e selecione **Acquire Now**.
3. Verifique se a aquisição é concluída com sucesso, sem erros.

   Para que a integração do Workflow Automation com o Unified Manager seja bem-sucedida, é necessário resolver os erros de aquisição.

Como a reinstalação ou atualização do OnCommand Workflow Automation afeta o Active IQ Unified Manager

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 atualmente em execução ou agendados sejam interrompidos.

Você também deve excluir manualmente o Unified Manager do OnCommand Workflow Automation.

Após reinstalar ou atualizar o OnCommand Workflow Automation, você deve configurar novamente a conexão com o Unified Manager.

Remova a configuração do OnCommand Workflow Automation do Active IQ 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 precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **General** > **Workflow Automation** no menu Setup à esquerda.
2. Na página **Workflow Automation**, clique em **Remove Setup**.

Execute um failover e failback de uma relação de proteção

Execute um failover e failback de uma relação de proteção no Active IQ Unified Manager

Quando um volume de origem em seu relacionamento de proteção é desativado devido a uma falha de hardware ou a 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 fique online novamente; em seguida, você pode retornar à origem original quando ela estiver disponível para fornecer dados.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o OnCommand Workflow Automation para executar esta operação.

Passos

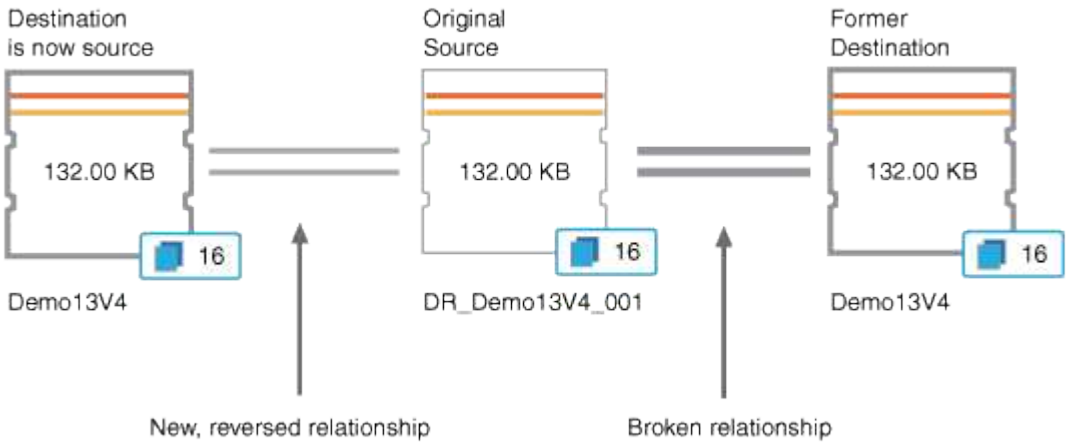
1. "Rompa a relação do SnapMirror".

   Você deve romper a relação antes de poder converter o destino de um volume de proteção de dados em um volume de leitura/gravação e antes de poder reverter a relação.

2. "Inverta a relação de proteção".

   Quando o volume de origem original estiver disponível novamente, você poderá optar por restabelecer a relação de proteção original restaurando o volume de origem. Antes de restaurar a origem, você deve sincronizá-la com os dados gravados no antigo destino. Você usa a operação de ressincronização reversa para criar uma nova relação de proteção, invertendo as funções da relação original e sincronizando o volume de origem com o antigo destino. Uma nova cópia Snapshot de linha de base é criada para a nova relação.

   A relação inversa é semelhante a uma relação em cascata:



3. "Quebre a relação do SnapMirror invertida".

   Quando o volume de origem original for ressincronizado e puder novamente fornecer dados, use a operação de interrupção para quebrar a relação invertida.

4. "Remova o relacionamento".

   Quando a relação inversa não for mais necessária, você deve removê-la antes de restabelecer a relação original.

5. "Ressincronizar a relação".

   Use a operação de ressincronização para sincronizar os dados da origem para o destino e restabelecer a relação original.

Interrompa uma relação de proteção do SnapMirror na página Volume/Saúde do Active IQ Unified Manager

Você pode romper uma relação de proteção na página Volume / Health details e interromper as transferências de dados entre um volume de origem e um volume de destino em uma relação do SnapMirror. Você pode romper uma relação 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 romper uma

relação do SnapVault.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

Passos

1. Na aba **Proteção** da página de detalhes **Volume / Saúde**, selecione na topologia a relação do SnapMirror que você deseja interromper.
2. Clique com o botão direito do mouse no destino e selecione **Break** no menu.

   A caixa de diálogo "Break Relationship" é exibida.

3. Clique em **Continuar** para interromper a relação.
4. Na topologia, verifique se a relação está rompida.

Reverta as relações de proteção na página de detalhes de Volume/Saúde no Active IQ Unified Manager

Quando um desastre desativa o volume de origem na sua relação de proteção, você pode usar o volume de destino para fornecer dados, convertendo-o em leitura/gravação enquanto repara ou substitui o volume de origem. Quando a origem estiver novamente disponível para receber dados, você pode usar a operação de ressincronização reversa para estabelecer a relação na direção inversa, sincronizando os dados na origem com os dados no destino de leitura/gravação.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.
- A relação não deve ser uma relação do SnapVault.
- Já deve existir uma relação de proteção.
- A relação de proteção deve ser rompida.
- 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 forem mais recentes do que os dados na cópia Snapshot comum serão excluídos.
- As políticas e os cronogramas criados na relação de ressincronização reversa são os mesmos da relação de proteção original.

  Se as políticas e os cronogramas não existirem, eles serão criados.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, localize na topologia a relação do SnapMirror na qual você deseja inverter a origem e o destino e clique nela com o botão direito do mouse.
2. Selecione **Reverse Resync** no menu.

   A caixa de diálogo "Reverse Resync" é exibida.

3. Verifique se o relacionamento exibido na caixa de diálogo **Reverse Resync** é aquele para o qual você deseja executar a operação de ressincronização inversa e clique em **Submit**.

   A caixa de diálogo "Reverse Resync" é fechada, e um link do trabalho é exibido na parte superior da página de detalhes Volume / Health.

4. **Opcional:** clique em **View Jobs** na página de detalhes **Volume / Health** para acompanhar o status de cada trabalho de ressincronização reversa.

   Uma lista filtrada de tarefas é exibida.

5. **Opcional:** clique na seta **Voltar** do seu navegador para retornar à página de detalhes de **Volume / Saúde**.

   A operação de ressincronização reversa é concluída quando todas as tarefas do trabalho são finalizadas com sucesso.

Remova uma relação de proteção da página Detalhes de Volume/Saúde em Active IQ Unified Manager

Você pode remover uma relação de proteção para excluir permanentemente uma relação existente entre a origem e o destino selecionados: por exemplo, quando quiser criar uma relação usando um destino diferente. Essa operação remove todos os metadados e não pode ser desfeita.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

Passos

1. Na aba **Proteção** da página de detalhes **Volume / Saúde**, selecione na topologia a relação do 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 a relação.

   A relação foi removida da página de detalhes de Volume / Health.

Ressincronize as relações de proteção na página de detalhes de Volume/Integridade no Active IQ Unified Manager

Você pode ressincronizar dados em uma relação do SnapMirror ou do SnapVault que foi interrompida e, em seguida, o destino foi configurado como leitura/gravação, para que os dados na origem correspondam aos dados no destino. Você também pode ressincronizar quando uma cópia Snapshot comum necessária no volume de origem é excluída, fazendo com que as atualizações do SnapMirror ou do SnapVault falhem.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o OnCommand Workflow Automation.

Passos

1. Na guia **Protection** da página de detalhes **Volume / Health**, localize na topologia a relação de proteção que você deseja ressincronizar e clique com o botão direito do mouse sobre ela.
2. Selecione **Resynchronize** no menu.

   Como alternativa, no menu **Ações**, selecione **Relacionamento** > **Ressincronizar** para ressincronizar o relacionamento cujos detalhes você está visualizando.

   A caixa de diálogo Ressincronizar é exibida.

3. Na aba **Opções de Ressincronização**, selecione uma prioridade de transferência e a taxa de transferência máxima.
4. Clique em **Cópias Snapshot de origem**; em seguida, na coluna **Cópia Snapshot**, clique em **Padrão**.

   A caixa de diálogo Selecionar cópia Snapshot de origem é exibida.

5. Se você quiser especificar uma cópia Snapshot existente em vez de transferir a cópia Snapshot padrão, clique em **Cópia Snapshot existente** e selecione uma cópia Snapshot na lista.
6. Clique em **Enviar**.

   Você retorna à caixa de diálogo Ressincronizar.

7. Se você selecionou mais de uma origem para ressincronizar, clique em **Default** para a próxima origem para a qual deseja especificar uma cópia Snapshot existente.
8. Clique em **Submit** para iniciar a tarefa de ressincronização.

   O trabalho de ressincronização é iniciado, você retorna à página de detalhes de Volume/Integridade e um link de tarefas é exibido na parte superior da página.

9. **Opcional:** clique em **Ver trabalhos** na página **Detalhes de volume/integridade** para acompanhar o status de cada trabalho de ressincronização.

   Uma lista filtrada de tarefas é exibida.

10. **Opcional:** clique na seta **Voltar** do seu navegador para retornar à página de detalhes de **Volume / Saúde**.

    O processo de ressincronização termina quando todas as tarefas do trabalho são concluídas com sucesso.

Resolver uma falha em uma tarefa de proteção

Resolver uma falha em uma tarefa de proteção no Active IQ Unified Manager

Este fluxo de trabalho fornece um exemplo de como você pode identificar e resolver uma falha em uma tarefa de proteção a partir do painel do Unified Manager.

Antes de começar

Como algumas tarefas neste fluxo de trabalho exigem que você faça login usando a função de Administrador, você precisa estar familiarizado com as funções necessárias para usar as diversas funcionalidades.

Nesse cenário, você acessa a página Dashboard para ver se há algum problema com suas tarefas de proteção. Na área Protection Incident, você percebe que há um incidente Job Terminated, mostrando um erro

Protection Job Failed em um volume. Você investiga esse erro para determinar a possível causa e a possível solução.

Passos

1. No painel "Incidentes de proteção" da área "Incidentes e riscos não resolvidos" do Dashboard, 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 de detalhes do evento para a tarefa de proteção com falha é exibida.

2. Analise a mensagem de erro no campo Cause da área **Summary** para determinar o problema e avaliar possíveis ações corretivas.

   Consulte "Identificar o problema e executar ações corretivas para uma falha na tarefa de proteção".

Identifique o problema e execute ações corretivas para uma tarefa de proteção com falha no Active IQ Unified Manager

Você analisa a mensagem de erro de falha da tarefa no campo Causa da página Detalhes do evento e determina que a tarefa falhou devido a um erro de cópia Snapshot. Em seguida, você acessa a página Detalhes do volume/integridade para obter mais informações.

Antes de começar

Você precisa ter a função de Application Administrator.

A mensagem de erro exibida no campo Causa da 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:

- Uma tarefa de backup ou espelhamento não foi concluída com êxito.

  A tarefa envolvia uma relação de proteção entre o volume de origem `cluster2_src_vol2` no servidor virtual `cluster2_src_svm` e o volume de destino `managed_svc2_vol3` no servidor virtual chamado `cluster3_dst_svm`.

- Um trabalho de cópia Snapshot falhou para `0426cluster2_src_vol2snap` no volume de origem `cluster2_src_svm:/cluster2_src_vol2`.

Nesse cenário, você pode identificar a causa e as possíveis ações corretivas da falha da tarefa. No entanto, para resolver a falha, você precisa acessar a interface 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 Snapshot falhou no volume de origem, indicando que provavelmente há um problema com o seu volume de origem.

   Opcionalmente, você poderia clicar no link **Job Details** no final da mensagem de erro, mas para os fins deste cenário, você opta por não fazer isso.

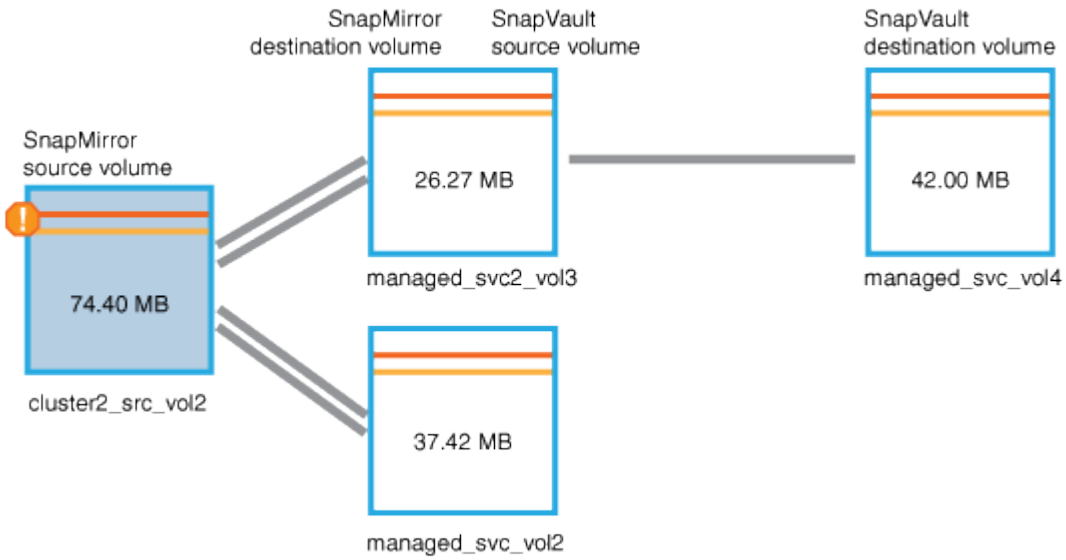
2. Você decide que quer tentar resolver o evento, então faz o seguinte:
   a. Clique no botão **Atribuir a** e selecione **Eu** do menu.
   b. Clique no botão **Acknowledge** para que você não continue recebendo notificações de alerta repetidas, caso alertas tenham sido configurados para o evento.
   c. Opcionalmente, você também pode adicionar notas sobre o evento.
3. Clique no campo **Origem** 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 Snapshot foi agendado.

   A página de detalhes Volume / Health é exibida para `cluster2_src_vol2`, mostrando o conteúdo da guia Protection.

4. Ao observar o gráfico da topologia de proteção, você verá um ícone de erro associado ao primeiro volume na topologia, que é o volume de origem para a relação do SnapMirror.

   Você também verá as barras horizontais no ícone do volume de origem, que indicam os limites de aviso e erro definidos para esse volume.



5. Ao posicionar o cursor sobre o ícone de erro, você vê a caixa de diálogo pop-up que exibe as configurações de limite e vê que o volume excedeu o limite de erro, o que indica um problema de capacidade.
6. Clique na guia **Capacidade**.

Informações sobre a capacidade das exibições de volume `cluster2_src_vol2`.

7. No painel **Capacidade**, você vê um ícone de erro no gráfico de barras, indicando novamente que a capacidade do volume ultrapassou o nível de limite definido para o volume.
8. Abaixo do gráfico de capacidade, você vê que o volume com crescimento automático foi desativado e que uma garantia de espaço do volume foi definida.

   Você poderia optar por ativar o crescimento automático, mas para os fins deste cenário, você decide investigar mais a fundo antes de tomar uma decisão sobre como resolver o problema de capacidade.

9. Ao rolar a página para baixo até a lista de **Eventos**, você vê que os eventos Protection Job Failed, Volume Days Until Full e Volume Space Full foram gerados.
10. Na lista **Events**, clique no evento **Volume Space Full** para obter mais informações, após decidir que esse evento parece ser o mais relevante para o seu problema de capacidade.

    A página de detalhes do evento exibe o evento "Volume Space Full" 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 de Resumo, você verá as ações corretivas sugeridas.

    As Ações Corretivas Sugeridas são exibidas apenas para alguns eventos, portanto você não verá essa área para todos os tipos de eventos.

    Você percorre a lista de ações sugeridas que pode executar para resolver o evento Volume Space Full:

    - Ative o crescimento automático neste volume.
    - Redimensione o volume.
    - Ative e execute a deduplicação neste volume.
    - Ative e execute a compressão neste volume.

13. Você decide habilitar o crescimento automático no volume, mas, para isso, precisa determinar o espaço livre disponível no agregado pai e a taxa de crescimento atual do volume:
    a. Observe o agregado pai, `cluster2_src_aggr1`, no painel **Related Devices**.

       Você pode clicar no nome do agregado para obter mais detalhes sobre o agregado.

       Você determina que o agregado tem espaço suficiente para habilitar o volume com crescimento automático.

    b. Na parte superior da página, observe o ícone que indica um incidente crítico e leia o texto abaixo do ícone.

       Você determina que "Dias para atingir a capacidade máxima: menos de um dia | Taxa de crescimento diário: 5,4%".

14. Acesse o System Manager ou a ONTAP CLI para habilitar a `volume autogrow` opção.

    Anote os nomes do volume e do agregado para tê-los disponíveis ao ativar o crescimento automático.

15. Após resolver o problema de capacidade, retorne à página de detalhes de **Evento** do Unified Manager e marque o evento como resolvido.

Resolva problemas de latência no Active IQ Unified Manager

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, caso existam, encontrar soluções.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Na página do Dashboard, você observa a área Incidentes e riscos não resolvidos e vê um erro de SnapMirror Lag no painel Proteção, em Riscos de proteção.

Passos

1. No painel **Proteção** da página **Painel de Controle**, localize o erro de atraso da relação do SnapMirror e clique nele.

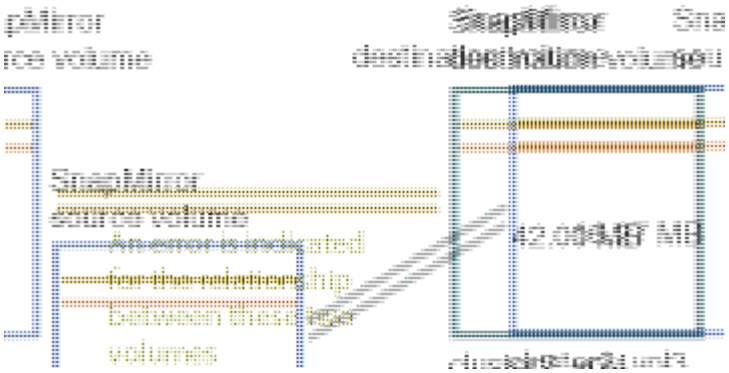
   A página de detalhes do evento para o evento de erro de atraso é exibida.

2. Na página de detalhes de **Event**, você pode realizar uma ou mais das seguintes tarefas:
   - Analise 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 Source da área Summary para obter detalhes sobre o volume.
   - Procure anotações 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. Nesse cenário, você clica no nome do objeto (nesse caso, um volume) no campo Origem da área **Resumo** para obter detalhes sobre o volume.

   A página Detalhes de Volume/Saúde exibe a aba Proteção.

4. Na aba **Proteção**, você visualiza o diagrama de topologia.

   Você observa que o volume com o erro de atraso é o último volume em uma cascata de SnapMirror de três volumes. O volume que você selecionou está contornado em cinza-escuro, e uma linha dupla laranja partindo do volume de origem indica um erro de relação do SnapMirror.



5. Clique em cada um dos volumes na cascata do SnapMirror.

   Ao selecionar cada volume, as informações de proteção nas áreas Resumo, Topologia, Histórico, Eventos, Dispositivos Relacionados e Alertas Relacionados mudam para exibir detalhes relevantes para o volume selecionado.

6. Você visualiza a área **Resumo** e posiciona o cursor sobre o ícone de informações no campo **Atualização Programada** para cada volume.

   Nesse cenário, você observa que a política SnapMirror é DPDefault e que o agendamento SnapMirror é atualizado de hora em hora, cinco minutos após a hora. Você percebe que todos os volumes na relação estão tentando concluir uma transferência SnapMirror ao mesmo tempo.

7. Para resolver o problema de atraso, você modifica os agendamentos de dois dos volumes em cascata, de forma que cada destino inicie uma transferência do SnapMirror depois que sua origem tiver concluído uma transferência.

Gerenciar e monitorar relações de proteção

Saiba como gerenciar e monitorar relações de proteção no Active IQ Unified Manager

O Active IQ Unified Manager permite que você crie relações de proteção, monitore e solucione problemas nas relações do SnapMirror e do SnapVault em clusters gerenciados, e restaure dados quando eles forem sobrescritos ou perdidos.

Para operações do SnapMirror, existem dois tipos de replicação:

- Assíncrono

  A replicação do volume primário para o volume secundário é determinada por um cronograma.

- Síncrono

  A replicação é realizada simultaneamente no volume primário e no volume secundário.

Você pode executar até 10 tarefas de proteção simultaneamente sem impacto no desempenho. Pode haver alguma queda de desempenho ao executar entre 11 e 30 tarefas simultaneamente. Não é recomendável executar mais de 30 tarefas simultaneamente.

Visualize o status da proteção de volume no Active IQ Unified Manager

A página de Proteção de Dados apresenta uma visão holística dos detalhes da proteção de dados para todos os volumes protegidos em um único cluster ou em todos os clusters de um data center.

Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Dependendo de você querer visualizar o status da 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 de Proteção de Dados. A página **Proteção de Dados** é exibida.

Dependendo de você ter selecionado um único cluster ou todos os clusters do seu data center, esta página exibe o status de proteção de dados dos volumes protegidos por cópias Snapshot ou políticas do SnapMirror, além de exibir a contagem de volumes desprotegidos.

Selecionar um cluster na lista **Individual Cluster** exibe o status da proteção do Snapshot e o status da relação do SnapMirror dos volumes protegidos nesse cluster.

Clicar nos eventos nesta página leva você à página de detalhes do evento. Você pode clicar no link **Ver tudo** para visualizar todos os eventos de proteção ativos na página de inventário de gerenciamento de eventos. Você pode passar o mouse para ver as respectivas contagens e legendas. Você pode clicar em:

- Os gráficos de barras de volumes desprotegidos e volumes protegidos por cópias Snapshot levam você à página Volumes, onde você pode ver os detalhes.
- Os gráficos de barras de todas as relações levam à página Relationships, onde os detalhes são filtrados pelo cluster de origem.

Visualizar o estado de proteção dos volumes protegidos por cópias Snapshot

Visão geral das cópias Snapshot: uma visão geral dos volumes protegidos por cópias Snapshot, tais como:

- O número total de volumes protegidos e não protegidos por cópias Snapshot.
- O número total de volumes que estão usando ou excedendo o espaço reservado para as cópias Snapshot.

Análise de cópias Snapshot detalha as seguintes informações:

- Eventos individuais para cópias Snapshot, incluindo os eventos ocorridos nas últimas 24 horas.
- Tabela detalhada dos volumes protegidos e não protegidos por cópias Snapshot.
- Volumes que usam, não usam e excedem a capacidade reservada para cópias Snapshot.
- Detalhamento da contagem de volumes em termos do número de suas cópias Snapshot.

Pontos a observar para cópias Snapshot

- Para contabilizar os volumes protegidos por cópias Snapshot, os volumes de origem e de destino são considerados.
- O número de cópias Snapshot retornadas refere-se apenas aos volumes que estão online e disponíveis.
- O intervalo do gráfico para o número de cópias Snapshot é dinâmico. Ele é gerado com base no número

de snapshots presentes no cluster selecionado.

- Para que um volume seja considerado protegido, o agendamento para a cópia Snapshot do volume deve estar ativado.
- O valor do espaço reservado para cópias Snapshot é importante para visualizar a quantidade de espaço de disco utilizado ou para calcular o espaço que pode ser recuperado caso uma ou mais cópias Snapshot sejam excluídas.

Exibir o status de proteção das relações do SnapMirror

SnapMirror Visão geral: uma visão geral dos volumes protegidos por políticas do SnapMirror, tais como:

- O número de volumes protegidos pelas respectivas políticas do SnapMirror, como relações do SnapMirror de volume, recuperação de desastres de máquinas virtuais de armazenamento (SVM-DR) e suas combinações.
- O número total de relações do SnapMirror que apresentam atraso no objetivo de ponto de recuperação (RPO) com base no status do atraso.

Análise do SnapMirror detalha as seguintes informações:

- Eventos individuais gerados para as relações 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 Espelho assíncrono, Cofre assíncrono, MirrorVault assíncrono, StricxtSync, grupo de consistência de sincronização ativa do SnapMirror e Sincronização.
- O número de relacionamentos saudáveis e não saudáveis.
- Detalhamento da contagem de relacionamento de volume. Você pode alternar os gráficos por tempo de atraso do RPO e status.
- Limiares de atraso para relacionamento não gerenciado. Você pode clicar no ícone de configurações ( ) para configurar as definições de limite de atraso. Para obter mais informações, consulte "Configurando as configurações de limite de atraso para relações de proteção não gerenciadas".

Pontos a serem observados para relações do SnapMirror

- Para contabilizar as relações do SnapMirror, são contados os volumes de origem habilitados para leitura e gravação. Os volumes de destino e raiz não são considerados.
- Para a relação do 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 de RPO na replicação de dados é baseada na relação do SnapMirror. O status é categorizado como `ok`, `warning`, ou `error`, com base no limite de relação definido. Você pode verificar o status para determinar se os parâmetros estão funcionando conforme o esperado ou se precisa resolver algum problema.
- Se um volume tiver vários relacionamentos do SnapMirror, cada tipo de relacionamento será contado para o atraso do RPO.
- As relações de volume são consideradas problemáticas se houver falhas na replicação de dados entre a origem e o destino, por exemplo, quando a relação é interrompida.

Visualizar clusters protegidos pela configuração do MetroCluster

O painel **Proteção do MetroCluster** na página **Data Protection** exibe o número de clusters protegidos ou não protegidos pela configuração FC ou IP do MetroCluster no seu site. Clicar nos gráficos de barras nesse 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 de configurações do MetroCluster".

Visualize as relações de proteção de volume no Active IQ Unified Manager

Na visualização Relacionamento: Todos os Relacionamentos e na página Relacionamentos de Volume, você pode ver o status das relações existentes do volume SnapMirror e SnapVault. Você também pode examinar detalhes sobre as relações de proteção, incluindo o status de transferência e de atraso, detalhes de origem e destino, informações de agendamento e política, entre outros.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Você também pode iniciar comandos de relacionamento a partir desta página.

Passos

1. No painel de navegação à esquerda, 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 do volume:

   - Para visualizar informações atuais sobre todos os relacionamentos de volume, permaneça na página padrão **All Relationships**.
   - Para visualizar informações detalhadas sobre as tendências de transferência de volume ao longo de um período, no menu Exibir, selecione Relacionamento: visualização do 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 apenas para volumes em relacionamentos assíncronos; os volumes em relacionamentos síncronos não são exibidos.

Monitorar os relacionamentos LUN do Consistency Group no Active IQ Unified Manager

Se o seu ambiente ONTAP oferecer suporte ao SnapMirror active sync para proteger aplicações com LUNs, você poderá visualizar e monitorar essas LUNs no Active IQ Unified Manager.

O SnapMirror active sync garante objetivo de tempo de recuperação (RTO) zero durante o failover em ambientes SAN. Em uma implantação típica com suporte ao SnapMirror active sync, os LUNs nos volumes são protegidos por relações de grupo de consistência.

Esses LUNs primários e secundários são LUNs compostos, ou seja, um par de LUNs de réplica com o mesmo UUID e número de série. As operações de E/S (tanto de leitura quanto de gravação) são multiplexadas entre os sites de origem e destino nesses LUNs compostos, garantindo transparência.

Para visualizar LUNs compostas, os clusters primário e secundário com as LUNs que fazem parte da relação do grupo de consistência devem ser adicionados e descobertos no Unified Manager. Somente LUNs iSCSI e FCP são compatíveis.

Para obter informações sobre a sincronização ativa do SnapMirror, consulte "Documentação do ONTAP 9 para a sincronização ativa do SnapMirror (anteriormente SM-BC)".

Para visualizar LUNs compostos em seu ambiente siga estas etapas:

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **LUNs**.
2. No menu Exibir, selecione **Relacionamento** > **Todos os LUNs**.

   A visualização "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 acessar uma visualização detalhada. Clicar no grupo de consistência leva você à página Relationships.

Ao clicar no LUN parceiro, você pode ver os detalhes de configuração dele na guia SAN da página Detalhes da VM de armazenamento da VM de armazenamento em que o LUN parceiro está hospedado. Informações como os iniciadores, os grupos de iniciadores e outros aspectos do LUN parceiro são exibidas.

Você pode executar as funções padrão no nível da grade, como classificar, filtrar, gerar e carregar relatórios para as LUNs protegidas em seu ambiente.

Crie uma relação do SnapVault a partir da visualização Saúde: Todos os Volumes em Active IQ Unified Manager

Você pode usar a visualização "Saúde: Todos os Volumes" para criar relações do SnapVault para um ou mais volumes na mesma VM de storage para habilitar backups de dados para fins de proteção.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

O menu **Proteger** não é exibido nos seguintes casos:

- Se as configurações do RBAC não permitirem essa ação: por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido: por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.

2. Na visualização **Saúde: todos os volumes**, selecione o volume que deseja proteger e clique em **Proteger**.

   Como alternativa, para criar várias relações de proteção na mesma máquina virtual de storage (SVM), selecione um ou mais volumes na visualização Integridade: todos os volumes e clique em **Proteger** na barra de ferramentas.

3. Selecione **SnapVault** no menu.

   A caixa de diálogo Configure Protection é aberta.

4. Clique em **SnapVault** para ver a guia **SnapVault** e configurar as informações do volume secundário.
5. Clique em **Avançado** para configurar a desduplicação, a compressão, 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 guia **SnapVault**.
7. Clique em **Aplicar**.

   Você retornará à visualização Saúde: todos os volumes.

8. Clique no link da tarefa de configuração de proteção na parte superior da visualização **Saúde: todos os volumes**.

   Se você estiver criando apenas uma relação de proteção, a página de detalhes da tarefa será exibida; no entanto, se estiver criando mais de uma relação de proteção, será exibida uma lista filtrada de todas as tarefas associadas à operação de proteção.

9. Faça um dos seguintes procedimentos:
   - Se você tiver apenas um trabalho, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho estará concluído.
   - Se você tiver mais de uma tarefa:
     i. Clique em uma tarefa na lista de tarefas.
     ii. Clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para verificar quando o trabalho for concluído.
     iii. Use o botão **Voltar** para retornar à lista filtrada e visualizar outra tarefa.

Crie uma relação de proteção do SnapVault na página de detalhes de Volume/Saúde do Active IQ Unified Manager

Você pode criar uma relação do SnapVault usando a página de detalhes de Volume / Health para que os backups de dados sejam ativados para fins de proteção nos volumes.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation para executar esta tarefa.

O menu **Proteger** não é exibido nos seguintes casos:

- Se as configurações do RBAC não permitirem essa ação: por exemplo, se você tiver apenas privilégios de

operador

- Quando o ID do volume é desconhecido: por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, clique com o botão direito do mouse em um volume na visualização da topologia que você deseja proteger.
2. Selecione **Proteger** > **SnapVault** no menu.

   A caixa de diálogo Configure Protection é aberta.

3. Clique em **SnapVault** para visualizar a guia **SnapVault** e configurar as informações do recurso secundário.
4. Clique em **Avançado** para configurar a desduplicação, a compressão, o crescimento automático e a garantia de espaço conforme necessário e, em seguida, clique em **Aplicar**.
5. Complete a área **Informações de destino** e a área **Configurações de relacionamento** na caixa de diálogo **Configurar proteção**.
6. Clique em **Aplicar**.

   Você retorna à página de detalhes Volume / Health.

7. Clique no link do trabalho de configuração da proteção na parte superior da página de detalhes **Volume / Health**.

   A página de detalhes do trabalho é exibida.

8. Clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para verificar quando o trabalho for concluído.

   Quando as tarefas do trabalho estiverem concluídas, os novos relacionamentos serão exibidos na exibição de topologia da página de detalhes Volume / Health.

Crie uma relação do SnapMirror a partir da visualização Saúde: Todos os Volumes no Active IQ Unified Manager

Usar a visualização "Saúde: todos os volumes" permite que você crie várias relações de proteção do SnapMirror ao mesmo tempo, selecionando mais de um volume na mesma máquina virtual de storage.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

O menu **Proteger** não é exibido nos seguintes casos:

- Se as configurações do RBAC não permitirem essa ação: por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido: por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

Passos

1. Na visualização **Saúde: todos os volumes**, selecione o volume que deseja proteger.

   Como alternativa, para criar várias relações de proteção no mesmo SVM, selecione um ou mais volumes na visualização Health: All Volumes e clique em **Protect** > **SnapMirror** na barra de ferramentas.

   A caixa de diálogo Configurar Proteção é exibida.

2. Clique em **SnapMirror** para visualizar a guia **SnapMirror** e configurar as informações de destino.
3. Clique em **Avançado** para definir a garantia de espaço, conforme necessário, e depois clique em **Aplicar**.
4. Preencha a área **Informações de destino** e a área **Configurações de relacionamento** na guia **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 **Health: All Volumes view**.

   Se você estiver criando apenas um relacionamento de proteção, verá a página de detalhes do trabalho; no entanto, se estiver criando mais de um relacionamento de proteção, verá uma lista de todos os trabalhos associados à operação de proteção.

7. Faça um dos seguintes procedimentos:
   - Se você tiver apenas um trabalho, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para determinar quando o trabalho estará concluído.
   - Se você tiver mais de uma tarefa:
     i. Clique em uma tarefa na lista de tarefas.
     ii. Clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e para verificar quando o trabalho for concluído.
     iii. Use o botão **Voltar** para retornar à lista filtrada e visualizar outra tarefa.

Dependendo da SVM de destino especificada durante a configuração ou das opções que você ativou nas suas configurações avançadas, a relação do SnapMirror resultante pode ser uma das várias variações possíveis:

- Se você especificou uma SVM de destino executada na mesma versão do ONTAP ou em uma versão mais recente que a do volume de origem, uma relação do SnapMirror baseada em replicação de blocos será o resultado padrão.
- Se você especificou uma SVM de destino que é executada na mesma versão ou em uma versão mais recente do ONTAP em comparação com a do volume de origem, mas habilitou a replicação flexível de versão nas configurações avançadas, o resultado é uma relação do SnapMirror com replicação flexível de versão.
- Se você especificou uma SVM de destino executada em uma versão do ONTAP anterior à do volume de origem, e a versão anterior oferece suporte à replicação flexível de versão, uma relação do SnapMirror com replicação flexível de versão é o resultado automático.

Crie uma relação do SnapMirror a partir da página de detalhes de integridade do volume no Active IQ Unified Manager

Você pode usar a página de detalhes de Volume/Integridade para criar uma relação do SnapMirror para que a replicação de dados seja habilitada para fins de proteção. A replicação do SnapMirror permite restaurar os dados do volume de destino em caso de perda de dados na origem.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

O menu **Proteger** não é exibido nos seguintes casos:

- Se as configurações do RBAC não permitirem essa ação: por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido: por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

Você pode executar até 10 tarefas de proteção simultaneamente sem impacto no desempenho. Pode haver alguma queda de desempenho ao executar entre 11 e 30 tarefas simultaneamente. Não é recomendável executar mais de 30 tarefas simultaneamente.

Passos

1. Na aba **Proteção** da página de detalhes **Volume / Saúde**, na visualização de topologia clique com o botão direito do mouse 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 guia **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. Complete a área **Informações de destino** e a área **Configurações de relacionamento** na caixa de diálogo **Configurar proteção**.
6. Clique em **Aplicar**.

   Você retorna à página de detalhes Volume / Health.

7. Clique no link do trabalho de configuração da proteção na parte superior da página de detalhes **Volume / Health**.

   As tarefas e os detalhes do trabalho são exibidos na página Job details.

8. Na página de detalhes do **Job**, clique em **Refresh** para atualizar a lista de tarefas e os detalhes das tarefas associados ao job de configuração de proteção e determinar quando o job estará concluído.
9. Quando as tarefas do trabalho estiverem concluídas, clique em **Back** no seu navegador para retornar à página de detalhes **Volume / Health**.

   A nova relação é exibida na visualização de topologia da página de detalhes Volume / Health.

Dependendo da SVM de destino especificada durante a configuração ou das opções que você ativou nas

suas configurações avançadas, a relação do SnapMirror resultante pode ser uma das várias variações possíveis:

- Se você especificou uma SVM de destino executada na mesma versão do ONTAP ou em uma versão mais recente que a do volume de origem, uma relação do SnapMirror baseada em replicação de blocos será o resultado padrão.
- Se você especificou uma SVM de destino que é executada na mesma versão ou em uma versão mais recente do ONTAP em comparação com a do volume de origem, mas habilitou a replicação flexível de versão nas configurações avançadas, o resultado é uma relação do SnapMirror com replicação flexível de versão.
- Se você especificou uma SVM de destino executada em uma versão anterior do ONTAP, ou em uma versão superior à do volume de origem, e a versão anterior oferecer suporte à replicação flexível de versão, uma relação do SnapMirror com replicação flexível de versão será o resultado automático.

Crie uma relação do SnapMirror com replicação flexível em relação à versão no Active IQ Unified Manager

Você pode criar uma relação do SnapMirror com replicação flexível de versão. A replicação flexível de versão permite implementar a proteção do SnapMirror mesmo que os volumes de origem e de destino sejam executados em versões diferentes do ONTAP.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.
- As SVMs de origem e de destino devem ter, cada uma, uma licença de SnapMirror ativada.
- As SVMs de origem e de destino devem ser executadas, cada uma, em uma versão do ONTAP que ofereça suporte à replicação com flexibilidade de versão.

O SnapMirror com replicação flexível de versão permite que você implemente a proteção do SnapMirror mesmo em ambientes de storage heterogêneo nos quais nem todo o storage está em execução em uma única versão do ONTAP; no entanto, as operações de espelhamento realizadas com o SnapMirror com replicação flexível de versão não são executadas tão rapidamente quanto seriam com a replicação de bloco tradicional do 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 de Volume/Saúde, clique com o botão direito do mouse na visualização de topologia que contém o nome de um volume que você deseja proteger e selecione **Proteger** > **SnapMirror** no menu.
    - Se estiver visualizando a tela "Saúde: todos os volumes", localize um volume que você deseja proteger e clique com o botão direito do mouse nele; em seguida, selecione **Proteger** > **SnapMirror** no menu. A caixa de diálogo "Configurar proteção" é exibida.
2. Clique em **SnapMirror** para visualizar a guia **SnapMirror**.
3. Complete a área **Informações de destino** e a área **Configurações de relacionamento** na caixa de diálogo **Configurar proteção**.

    Se você especificar uma SVM de destino executada em uma versão anterior do ONTAP em relação ao volume de origem que você está protegendo, e se essa versão anterior oferecer suporte à replicação flexível de versão, esta tarefa configurará automaticamente o SnapMirror com replicação flexível de

versão.

4. Se você especificar uma SVM de destino que execute a mesma versão do ONTAP que a do volume de origem, mas ainda quiser configurar o SnapMirror com replicação flexível de versão, clique em **Avançado** para ativar a replicação flexível de versão e, em seguida, clique em **Aplicar**.
5. Clique em **Aplicar**.

   Você retorna à página de detalhes Volume / Health.

6. Clique no link do trabalho de configuração da proteção na parte superior da página de detalhes **Volume / Health**.

   As tarefas e os detalhes dos jobs são exibidos na página Job details.

7. Na página de detalhes do **Job**, clique em **Refresh** para atualizar a lista de tarefas e os detalhes das tarefas associados ao job de configuração de proteção e determinar quando o job estará concluído.
8. Quando as tarefas do trabalho estiverem concluídas, clique em **Back** no seu navegador para retornar à página de detalhes **Volume / Health**.

   A nova relação é exibida na visualização de topologia da página de detalhes Volume / Health.

Crie relações do SnapMirror com replicação flexível em relação à versão e capacidade de opção de reversão no Active IQ Unified Manager

Você pode criar uma relação do SnapMirror com replicação flexível em termos de versão e capacidade da opção de backup. A capacidade da opção de backup permite que você implemente a proteção do SnapMirror e também retenha várias versões de cópias de backup no local de destino.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.
- As SVMs de origem e de destino devem ter, cada uma, uma licença de SnapMirror ativada.
- As SVMs de origem e de destino devem ter, cada uma, uma licença de SnapVault ativada.
- As SVMs de origem e de destino devem ser executadas, cada uma, em uma versão do ONTAP que ofereça suporte à replicação com flexibilidade de versão.

Configurar o SnapMirror com a capacidade da opção de backup permite proteger seus dados com os recursos de recuperação de desastres do SnapMirror, como a capacidade de failover de volume, e, ao mesmo tempo, fornecer os recursos do SnapVault, como proteção com 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 na página de detalhes de Volume / Health, clique com o botão direito do mouse, na visualização de topologia, no nome de um volume que você deseja proteger e selecione **Protect** > **SnapMirror** no menu.
   - Se você estiver visualizando a tela "Saúde: todos os volumes", localize o volume que deseja proteger e clique nele com o botão direito do mouse; em seguida, selecione **Proteger** > **SnapMirror** no menu. A caixa de diálogo "Configurar proteção" é exibida.

2. Clique em **SnapMirror** para visualizar a guia **SnapMirror**.
3. Complete 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 **Replicação Flexível por Versão** ainda não estiver marcada, marque-a agora.
6. Selecione a caixa de seleção **Com opção de backup** para ativar a funcionalidade da opção de backup; em seguida, clique em **Aplicar**.
7. Clique em **Aplicar**.

   Você retorna à página de detalhes Volume / Health.

8. Clique no link do trabalho de configuração da proteção na parte superior da página de detalhes **Volume / Health**.

   As tarefas e os detalhes dos jobs são exibidos na página Job details.

9. Na página de detalhes da **Tarefa**, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e determinar quando o trabalho é concluído.
10. Quando as tarefas do trabalho estiverem concluídas, clique em **Back** no seu navegador para retornar à página de detalhes **Volume / Health**.

    A nova relação é exibida na visualização de topologia da página de detalhes Volume / Health.

Configure as configurações de eficiência do destino no Active IQ Unified Manager

Você pode configurar as configurações de eficiência do destino, como deduplicação, compactação, crescimento automático e garantia de espaço, em um destino de proteção usando a caixa de diálogo Configurações avançadas de destino. Você usa essas configurações quando quiser maximizar a utilização do espaço em um destino ou volume secundário.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Por padrão, as configurações de eficiência correspondem às do volume de origem, exceto as configurações de compressão em uma relação do SnapVault, que são desativadas por padrão.

Passos

1. Na caixa de diálogo **Configurar Proteção**, clique na guia **SnapMirror** ou na guia **SnapVault**, dependendo do tipo de relacionamento que você está configurando.
2. Clique em **Avançado** na área **Informações sobre o destino**.

   A caixa de diálogo Configurações avançadas de destino é aberta.

3. Ative ou desative as configurações de eficiência para desduplicação, compactação, crescimento automático e garantia de espaço, conforme necessário.
4. Clique em **Aplicar** para salvar suas seleções e voltar à caixa de diálogo **Configurar proteção**.

Crie agendas de SnapMirror e SnapVault no Active IQ Unified Manager

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 mudam em seus volumes.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você já deve ter preenchido a área Informações de destino na caixa de diálogo Configurar proteção.
- Você precisa ter configurado o Workflow Automation para executar esta tarefa.

Passos

1. Na guia **SnapMirror** ou na guia **SnapVault** da caixa de diálogo **Configurar proteção**, clique no link **Criar agendamento** na área **Configurações de relacionamento**.

   A caixa de diálogo Criar Agendamento é exibida.

2. No campo **Nome do Agendamento**, digite o nome que você deseja dar ao agendamento.
3. Selecione uma das seguintes opções:
   - **Básico**

     Selecione se você deseja criar um agendamento básico no estilo de intervalos.

   - **Avançado**

     Selecione se você deseja criar um agendamento no estilo cron.

4. Clique em **Create**.

   O novo horário é exibido na lista suspensa Schedule do SnapMirror ou Schedule do SnapVault.

Amplie a proteção usando relações em cascata ou ramificação no Active IQ Unified Manager

Você pode estender a proteção de um relacionamento existente criando um desdobramento (fan-out) a partir do volume de origem ou uma cascata (cascade) a partir do volume de destino de um relacionamento existente. Isso pode ser útil quando você precisa copiar dados de um site para vários sites ou fornecer proteção adicional criando mais backups.

Você pode estender a proteção a volumes usando o grupo de consistência, que é um contêiner que contém vários volumes para que você possa gerenciar todos os volumes como uma única entidade. Você pode visualizar o Grupo de consistência de sincronização ativa do SnapMirror e a relação de grupo de consistência síncrona na página Relacionamentos do Unified Manager.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

Passos

1. Clique em **Proteção** > **Relacionamentos**. Como alternativa, você pode visualizar os relacionamentos na página de detalhes do volume.
2. Na página **Relações de Volume**, selecione a relação do SnapMirror da qual você deseja estender a proteção.
3. Na barra de ações, clique em **Extend Protection**.
4. No menu, selecione **Da origem** ou **Do destino**, dependendo de você estar criando uma relação de fanout a partir da origem ou uma relação em cascata a partir do destino.
5. Selecione **Com SnapMirror** ou **Com SnapVault** dependendo do tipo de relação de proteção que você está criando.

   A caixa de diálogo **Configure Protection** é exibida.

   Isso pode ser feito na página de detalhes unified relationship / Volume Relationship e Volume / Health.

6. Preencha as informações conforme indicado na caixa de diálogo **Configurar Proteção**.

Edite as relações de proteção na página "Relações de Volume" no Active IQ Unified Manager

Você pode editar as relações de proteção existentes para alterar a taxa máxima de transferência, a política de proteção ou o agendamento de proteção. Você pode editar uma relação para diminuir a largura de banda usada para transferências ou para aumentar a frequência de transferências agendadas, visto que os dados são alterados com frequência.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Os volumes selecionados devem ser destinos de relacionamentos de proteção. Não é possível editar relacionamentos quando volumes de origem, volumes de balanceamento de carga ou volumes que não sejam o destino de uma relação do SnapMirror ou do SnapVault estiverem 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 Edit Relationship é exibida.

2. Na caixa de diálogo **Editar relacionamento**, edite a taxa de transferência máxima, a política de proteção ou o cronograma de proteção, conforme necessário.
3. Clique em **Aplicar**.

   As alterações são aplicadas aos relacionamentos selecionados.

Edite as relações de proteção na página Detalhes de Volume/Saúde no Active IQ Unified Manager

Você pode editar as relações de proteção existentes para alterar a taxa máxima de transferência atual, a política de proteção ou o agendamento de proteção. Você pode editar uma relação para diminuir a largura de banda usada para transferências ou para aumentar a frequência das transferências agendadas porque os dados mudam com frequência.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter instalado e configurado o Workflow Automation.

Os volumes selecionados devem ser destinos de relacionamentos de proteção. Não é possível editar relacionamentos quando volumes de origem, volumes de balanceamento de carga ou volumes que não sejam o destino de uma relação do SnapMirror ou do SnapVault estiverem selecionados.

Passos

1. Na guia **Protection** da página de detalhes **Volume / Health**, localize na topologia a relação de proteção que você deseja editar e clique nela com o botão direito do mouse.
2. Selecione **Editar** no menu.

   Alternativamente, no menu **Ações**, selecione **Relacionamento** > **Editar** para editar o relacionamento cujos detalhes você está visualizando.

   A caixa de diálogo **Edit Relationship** 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 do SnapMirror para maximizar a eficiência de transferência no Active IQ Unified Manager

Você pode criar uma política de SnapMirror para especificar a prioridade de transferência do SnapMirror para relações de proteção. As políticas de SnapMirror permitem maximizar a eficiência da transferência da origem para o destino, atribuindo prioridades para que as transferências de menor prioridade sejam agendadas para ser executadas após as transferências de prioridade normal.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.
- Esta tarefa pressupõe que você já tenha concluído a área Destination Information na caixa de diálogo Configure Protection.

Passos

1. Na guia **SnapMirror** da caixa de diálogo **Configurar proteção**, clique no link **Criar política** na área **Configurações de relacionamento**.

   A caixa de diálogo Criar Política de SnapMirror é exibida.

2. No campo **Nome da Política**, digite o nome que 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 **Create**.

   A nova política é exibida na lista suspensa Política do SnapMirror.

Crie uma política do SnapVault para maximizar a eficiência de transferência no Active IQ Unified Manager

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 uma relação de proteção.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.
- Você já deve ter concluído a área Destination Information na caixa de diálogo Configure Protection.

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 **Create**.

   A nova política é exibida na lista suspensa Criar Política.

Cancelar uma transferência na página Relações de Volume em Active IQ Unified Manager

Você pode abortar uma transferência ativa de proteção de dados quando quiser interromper uma replicação do SnapMirror que está em andamento. Você também pode limpar o ponto de verificação de reinicialização para transferências subsequentes à transferência completa. Você pode abortar uma transferência quando ela entrar em conflito com outra operação, como a movimentação de um volume.

Você não pode abortar relacionamentos de volumes protegidos pelo grupo de consistência.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

A ação de abortar não é exibida nos seguintes casos:

- Se as configurações do RBAC não permitirem essa ação: por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido: por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

Não é possível limpar o ponto de verificação de reinicialização de uma transferência completa.

Passos

1. Para cancelar transferências de uma ou mais relações de proteção, na página **Volume Relationships**, selecione um ou mais volumes e, na barra de ferramentas, clique em **Abort**.

   A caixa de diálogo Abort Transfer é exibida.

2. Se você quiser limpar o ponto de verificação de reinicialização de uma transferência que não seja uma transferência completa, selecione **Limpar pontos de verificação**.
3. Clique em **Continuar**.

   A caixa de diálogo Abort Transfer é fechada, e o status da tarefa de cancelamento é exibido na parte superior da página Volume Relationships, juntamente com um link para os detalhes da tarefa.

4. **Opcional:** Clique no link **View details** para acessar a página de detalhes do **Job** e ver detalhes adicionais e o andamento do job.

Cancelar uma transferência na página de detalhes de Volume/Saúde no Active IQ Unified Manager

Você pode abortar uma transferência ativa de proteção de dados quando quiser interromper uma replicação do SnapMirror em andamento. Você também pode limpar o ponto de verificação de reinício de uma transferência, caso não seja uma transferência completa. Você pode abortar uma transferência quando ela entrar em conflito com outra operação, como a movimentação de um volume.

Você não pode abortar relacionamentos de volumes protegidos pelo grupo de consistência.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

A ação de abortar não é exibida nos seguintes casos:

- Se as configurações do RBAC não permitirem essa ação: por exemplo, se você tiver apenas privilégios de operador

- Quando o ID do volume é desconhecido: por exemplo, quando você tem uma relação entre clusters e o cluster de destino ainda não foi descoberto

Não é possível limpar o ponto de verificação de reinicialização de uma transferência completa.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Health**, clique com o botão direito do mouse na relação na visualização de topologia da transferência de dados que você deseja abortar e selecione **Abortar**.

   A caixa de diálogo Abort Transfer é exibida.

2. Se você quiser limpar o ponto de verificação de reinicialização de uma transferência que não seja uma transferência completa, selecione **Limpar pontos de verificação**.
3. Clique em **Continuar**.

   A caixa de diálogo Abortar Transferência é fechada, e o status da operação de cancelamento é exibido na parte superior da página de detalhes de Volume / Integridade, juntamente com um link para os detalhes do trabalho.

4. **Opcional:** Clique no link **View details** para acessar a página de detalhes do **Job** e ver detalhes adicionais e o andamento do job.
5. Clique em cada tarefa para visualizar os detalhes.
6. Clique na seta de voltar do seu navegador para retornar à página de detalhes **Volume / Saúde**.

   A operação de cancelamento é finalizada quando todas as tarefas do trabalho forem concluídas com sucesso.

Suspenda uma relação de proteção na página Relações de Volume no Active IQ Unified Manager

Na página Relações de Volume, você pode suspender temporariamente uma relação de proteção para impedir que ocorram transferências de dados. Você pode suspender uma relação quando quiser criar uma cópia Snapshot de um volume de destino do SnapMirror que contenha um banco de dados e quiser garantir que seu conteúdo permaneça estável durante a operação de cópia Snapshot.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

A ação de quiescência não é exibida nos seguintes casos:

- Se as configurações do RBAC não permitirem essa ação; por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido; por exemplo, quando existe uma relação entre clusters e o cluster de destino ainda não foi descoberto
- Quando você não tiver emparelhado o Workflow Automation e o Unified Manager

Passos

1. Para suspender as transferências de uma ou mais relações de proteção, na página **Relações de Volume**,

selecione um ou mais volumes e, na barra de ferramentas, clique em **Suspender**.

A caixa de diálogo Quiesce é exibida.

2. Clique em **Continuar**.

   O status da tarefa de quiesce é exibido na parte superior da página de detalhes de Volume / Health, juntamente com um link para os detalhes da tarefa.

3. Clique no link **View details** para acessar a página de detalhes de **Job** e obter detalhes adicionais e acompanhar o andamento do trabalho.
4. **Opcional:** clique na seta **Voltar** do seu navegador para retornar à página **Relações de Volume**.

   O trabalho de quiescência é concluído quando todas as tarefas do trabalho são concluídas com sucesso.

Suspenda uma relação de proteção na página de detalhes de Volume/Saúde no Active IQ Unified Manager

Você pode suspender temporariamente uma relação de proteção para impedir que as transferências de dados ocorram. Você pode suspender uma relação quando quiser criar uma cópia Snapshot de um volume de destino do SnapMirror que contenha um banco de dados e quiser garantir que seu conteúdo permaneça estável durante a cópia Snapshot.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

A ação de quiescência não é exibida nos seguintes casos:

- Se as configurações do RBAC não permitirem essa ação, por exemplo, se você tiver apenas privilégios de operador
- Quando o ID do volume é desconhecido, por exemplo, quando existe uma relação entre clusters e o cluster de destino ainda não foi descoberto
- Quando você não tiver emparelhado o Workflow Automation e o Unified Manager

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Health**, clique com o botão direito do mouse na relação, na visualização de topologia, da relação de proteção que você deseja colocar em quiesce.
2. Selecione **Quiesce** no menu.
3. Clique em **Yes** para continuar.

   O status da tarefa de quiesce é exibido na parte superior da página de detalhes de Volume / Health, juntamente com um link para os detalhes da tarefa.

4. Clique no link **View details** para acessar a página de detalhes de **Job** e obter detalhes adicionais e acompanhar o andamento do trabalho.
5. **Opcional:** clique na seta Voltar do seu navegador para retornar à página de detalhes de **Volume / Health**.

   O trabalho de quiescência é concluído quando todas as tarefas do trabalho são concluídas com sucesso.

Desfaça uma relação do SnapMirror na página Relacionamentos de Volume do Active IQ Unified Manager

Você pode romper uma relação de proteção para interromper as transferências de dados entre um volume de origem e um volume de destino em uma relação do SnapMirror. Você pode romper uma relação 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 romper uma relação do SnapVault.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

Passos

1. Na página **Volume Relationships**, selecione um ou mais volumes com relações de proteção para os quais você deseja interromper as transferências de dados e, na barra de ferramentas, clique em **Break**.

   A caixa de diálogo "Break Relationship" é exibida.

2. Clique em **Continuar** para interromper a relação.
3. Na página **Relacionamentos de Volume**, verifique na coluna **Estado do Relacionamento** se o relacionamento está rompido.

   A coluna "Estado do Relacionamento" está oculta por padrão, portanto talvez seja necessário selecioná-la na lista de colunas a serem exibidas/ocultadas .

Remova uma relação de proteção da página Relações de Volume em Active IQ Unified Manager

Na página Relações de Volume, você pode remover uma relação de proteção para excluir permanentemente uma relação existente entre a origem e o destino selecionados: por exemplo, quando você deseja criar uma relação usando um destino diferente. Essa operação remove todos os metadados e não pode ser desfeita.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

Passos

1. Na página **Volume Relationships**, selecione um ou mais volumes com relações de proteção que você deseja remover e, na barra de ferramentas, clique em **Remove**.

   A caixa de diálogo Remover relacionamento é exibida.

2. Clique em **Continuar** para remover a relação.

   A relação foi removida da página Relações de volume.

Retome as transferências agendadas em uma relação inativa na página "Relacionamentos de Volume" no Active IQ Unified Manager

Depois de interromper uma relação para impedir que ocorram transferências agendadas, você pode usar **Resume** para reativá-las, de modo que os dados no volume de origem ou primário fiquem protegidos. As transferências são retomadas a partir de um ponto de verificação, se houver, no próximo intervalo de transferência agendado.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

Você pode selecionar no máximo 10 relacionamentos em pausa para retomar as transferências.

Passos

1. Na página **Relações** entre volumes, selecione um ou mais volumes com relações suspensas e, na barra de ferramentas, clique em **Retomar**.
2. Na caixa de diálogo **Retomar**, clique em **Continuar**.

   Você retorna à página Relações de volume.

3. Para ver as tarefas relacionadas e acompanhar o andamento delas, clique no link do trabalho exibido na parte superior da página **Volume Relationships**.
4. Faça um dos seguintes procedimentos:
   - Se apenas um trabalho for exibido, na página Detalhes do trabalho, clique em **Atualizar** para atualizar a lista de tarefas e os detalhes da tarefa associados ao trabalho de configuração de proteção e determinar quando o trabalho será concluído.
   - Se mais de um trabalho for exibido,
     i. Na página Jobs, clique no job cujos detalhes você deseja visualizar.
     ii. Na página Detalhes do job, clique em **Refresh** para atualizar a lista de tarefas e os detalhes da tarefa associados ao job de configuração de proteção e determinar quando o job é concluído. Depois que os jobs terminarem, as transferências de dados serão retomadas no próximo intervalo de transferência agendado.

Retome transferências em uma relação do SnapMirror inativa a partir da página de detalhes de Volume/Saúde no Active IQ Unified Manager

Após interromper uma relação para impedir que ocorram transferências agendadas, você pode usar **Retomar** na página de detalhes Volume / Health para reativar as transferências agendadas, de modo que os dados no volume de origem ou primário permaneçam protegidos. As transferências são retomadas a partir de um ponto de verificação, se houver, no próximo intervalo de transferência agendado.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, na visualização de topologia, clique com o botão direito do mouse em uma relação em pausa que você deseja retomar.

   Como alternativa, selecione **Retomar** no menu **Ações** > **Relacionamento**.

2. Na caixa de diálogo **Retomar**, clique em **Continuar**.

   Você retorna à página de detalhes Volume / Health.

3. Para visualizar as tarefas relacionadas e acompanhar o progresso delas, clique no link da tarefa exibido na parte superior da página de detalhes **Volume / Health**.
4. Na página de detalhes do **Job**, clique em **Refresh** para atualizar a lista de tarefas e os detalhes das tarefas associados ao job de configuração de proteção e determinar quando o job estará concluído.

   Após a conclusão das tarefas, as transferências de dados são retomadas no próximo intervalo de transferência agendado.

Inicialize ou atualize as relações de proteção na página Relações de Volume do Active IQ Unified Manager

Na página "Relacionamentos de Volume", você pode realizar uma primeira transferência completa em um novo relacionamento de proteção ou atualizar um relacionamento se ele já estiver inicializado e você quiser realizar uma atualização incremental manual, não agendada, para transferir os dados imediatamente.

Não é possível inicializar ou atualizar volumes protegidos por grupos de consistência.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o OnCommand Workflow Automation.

Passos

1. Na página **Relações de Volume**, clique com o botão direito em um volume e selecione um ou mais volumes com relações 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 Snapshot de origem**; em seguida, na coluna **Cópia Snapshot**, clique em **Padrão**.

   A caixa de diálogo Selecionar cópia Snapshot de origem é exibida.

4. Se você quiser especificar uma cópia Snapshot existente em vez de transferir a cópia Snapshot padrão, clique em **Cópia Snapshot existente** e selecione uma cópia Snapshot na lista.
5. Clique em **Enviar**.

   Você retorna à caixa de diálogo **Inicializar/Atualizar**.

6. Se você selecionou mais de uma origem para inicializar ou atualizar, clique em **Default** para a próxima

origem para a qual deseja especificar uma cópia Snapshot existente.

7. Clique em **Enviar** para iniciar a tarefa de inicialização ou atualização.

   A tarefa de inicialização ou atualização é iniciada, você retorna à página Relações de volume e um link para tarefas é exibido na parte superior da página.

8. **Opcional:** clique em **View Jobs** na visualização **Health: All Volumes** para acompanhar o status de cada tarefa de inicialização ou atualização.

   Uma lista filtrada de tarefas é exibida.

9. **Opcional:** clique em cada tarefa para ver seus detalhes.
10. **Opcional:** clique na seta **Voltar** do seu navegador para retornar à página **Relações de Volume**.

    A operação de inicialização ou atualização é concluída quando todas as tarefas forem concluídas com êxito.

Inicialize ou atualize as relações de proteção na página de detalhes de Volume/Integridade no Active IQ Unified Manager

Você pode realizar uma transferência completa em uma nova relação de proteção ou atualizar uma relação já inicializada, caso queira realizar uma atualização incremental manual e não programada para transferir os dados imediatamente.

NOTA: não é possível inicializar ou atualizar volumes protegidos por Consistency Groups.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o OnCommand Workflow Automation.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, localize na topologia a relação de proteção que deseja inicializar ou atualizar e clique com o botão direito do mouse sobre ela.
2. Selecione **Inicializar/Atualizar** no menu.

   Como alternativa, no menu **Ações**, selecione **Relação** > **Inicializar/Atualizar** para inicializar ou atualizar a relação cujos detalhes você está visualizando.

   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 Snapshot de origem**; em seguida, na coluna **Cópia Snapshot**, clique em **Padrão**.

   A caixa de diálogo Selecionar cópia Snapshot de origem é exibida.

5. Se você quiser especificar uma cópia Snapshot existente em vez de transferir a cópia Snapshot padrão, clique em **Cópia Snapshot existente** e selecione uma cópia Snapshot na lista.
6. Clique em **Enviar**.

   Você retorna 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 Snapshot existente.

   Não é possível selecionar uma cópia Snapshot diferente para volumes de proteção de dados.

8. Clique em **Enviar** para iniciar a tarefa de inicialização ou atualização.

   A tarefa de inicialização ou atualização é iniciada, você retorna à página de detalhes de Volume / Integridade e um link de tarefas é exibido na parte superior da página.

9. **Opcional:** Clique em **Visualizar Tarefas** na página de detalhes **Volume / Saúde** para acompanhar o status de cada tarefa de inicialização ou atualização.

   Uma lista filtrada de tarefas é exibida.

10. **Opcional:** clique em cada tarefa para ver seus detalhes.
11. **Opcional:** clique na seta Voltar do seu navegador para retornar à página de detalhes de **Volume / Health**.

    A operação de inicialização ou atualização é concluída quando todas as tarefas do trabalho são concluídas com êxito.

Ressincronize as relações de proteção na página "Relações de Volume" no Active IQ Unified Manager

Na página Relações de Volume, você pode ressincronizar uma relação para se recuperar de um evento que desativou seu volume de origem ou quando desejar alterar a origem atual para um volume diferente.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

Passos

1. Na página **Relações de Volume**, selecione um ou mais volumes com relações suspensas 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 de transferência máxima.
3. Clique em **Cópias Snapshot de origem**; em seguida, na coluna **Cópia Snapshot**, clique em **Padrão**.

   A caixa de diálogo Selecionar cópia Snapshot de origem é exibida.

4. Se você quiser especificar uma cópia Snapshot existente em vez de transferir a cópia Snapshot padrão, clique em **Cópia Snapshot existente** e selecione uma cópia Snapshot na lista.
5. Clique em **Enviar**.

   Você retorna à caixa de diálogo Ressincronizar.

6. Se você selecionou mais de uma origem para ressincronizar, clique em **Default** para a próxima origem para a qual deseja especificar uma cópia Snapshot existente.

7. Clique em **Submit** para iniciar a tarefa de ressincronização.

   A tarefa de ressincronização é iniciada, e você retorna à página Relações de volume, e um link para tarefas é exibido na parte superior da página.

8. **Opcional:** clique em **Visualizar Tarefas** na página **Relações de Volume** para acompanhar o status de cada tarefa de ressincronização.

   Uma lista filtrada de tarefas é exibida.

9. **Opcional:** clique na seta **Voltar** do seu navegador para retornar à página **Relações de Volume**.

   A operação de ressincronização termina quando todas as tarefas do trabalho são concluídas com sucesso.

Reverta as relações de proteção na página "Relações de Volume" no Active IQ Unified Manager

Quando um desastre desabilita o volume de origem em sua relação 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 pode usar a operação de ressincronização reversa para restabelecer a relação na direção inversa, sincronizando os dados na origem com os dados no destino de leitura/gravação.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.
- A relação não deve ser uma relação do SnapVault.
- Já deve existir uma relação de proteção.
- A relação de proteção deve ser rompida.
- 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 forem mais recentes do que os dados na cópia Snapshot comum serão excluídos.
- As políticas e os agendamentos criados em relacionamentos de ressincronização reversa são os mesmos do relacionamento de proteção original.

  Se as políticas e os cronogramas não existirem, eles serão criados.

Passos

1. Na página **Relações de Volume**, selecione um ou mais volumes com relações que você deseja reverter e, na barra de ferramentas, clique em **Reverter a ressincronização**.

   A caixa de diálogo "Reverse Resync" é exibida.

2. Verifique se os relacionamentos exibidos na caixa de diálogo **Reverse Resync** são aqueles para os quais você deseja executar a operação de ressincronização reversa e, em seguida, clique em **Submit**.

A operação de ressincronização reversa é iniciada, você retorna à página Relações de Volume e um link de tarefas aparece na parte superior da página.

3. **Opcional:** clique em **Visualizar tarefas** na página **Relações de volume** para acompanhar o status de cada tarefa de ressincronização reversa.

   Uma lista filtrada de trabalhos relacionados a esta operação é exibida.

4. **Opcional:** clique na seta **Voltar** do seu navegador para retornar à página **Relações de Volume**.

   A operação de ressincronização reversa é concluída quando todas as tarefas do trabalho são concluídas com sucesso.

Restaure os dados usando as páginas de detalhes de Volume e Volume/Integridade em Active IQ Unified Manager

Você pode restaurar arquivos, diretórios ou um volume inteiro sobrescritos ou excluídos de uma cópia Snapshot usando o recurso de restauração nas páginas de detalhes Volume e Volume / Health.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Observe os seguintes pontos:

- Não é possível restaurar um diretório ou um volume a partir de um snapshot em nenhum dos seguintes cenários:
  - A opção **Sim, preservar todas as cópias instantâneas** está selecionada.
  - Você está usando uma conta LDAP para monitorar o cluster.
  - Você está conectado como um usuário de domínio.
  - Sua conta está configurada para autenticação SAML.
  - Você está usando o protocolo NDMP.

    Para obter mais detalhes, consulte o artigo da Knowledge Base "Como configurar autenticação NDMP no modo 'SVM-scope'".
- 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 existe uma relação entre clusters e o cluster de destino ainda não foi descoberto.
  - O volume está configurado para a replicação síncrona do SnapMirror.

Passos

1. No painel de navegação esquerdo, acesse **Armazenamento > Volumes**.
2. Selecione o volume e clique no botão **Restaurar**. Como alternativa, clique no volume para acessar **Detalhes do Volume/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 Snapshot a partir dos quais você deseja restaurar os dados, caso sejam

diferentes dos padrões.

4. Selecione os itens que deseja restaurar, por exemplo, o LUN de origem.

   Você pode restaurar o volume inteiro ou especificar as pastas e os arquivos que deseja restaurar.

5. Selecione o local para o qual deseja restaurar os itens selecionados: **local original** ou **local alternativo existente**.
6. Se você selecionar um local alternativo já existente, faça um dos seguintes procedimentos:
   - No campo de texto "Caminho de restauração", digite o caminho do local para o qual você deseja restaurar os dados e clique em **Select Directory**.
   - Clique em **Procurar** para abrir a caixa de diálogo Procurar diretórios e conclua as seguintes etapas:
     i. Selecione o cluster de destino, a máquina virtual de armazenamento (SVM) e o volume para os quais você deseja restaurar.
     ii. Na tabela Name, selecione um nome de diretório que precisa ser restaurado.
     iii. Clique em **Select Directory**.
7. Clique em **Restaurar**.

   O processo de restauração começa. Uma tarefa é criada no backend para concluir o processo de restauração.

8. Se você quiser visualizar o progresso da tarefa, no painel de navegação esquerdo, acesse **Protection > Jobs** para visualizar o status da tarefa de restauração na lista de tarefas.

> Se uma operação de restauração falhar entre clusters HA do Cloud Volumes ONTAP com um erro de NDMP, talvez seja necessário adicionar uma rota AWS explícita no cluster de destino para que o destino possa se comunicar com a LIF de gerenciamento de cluster do sistema de origem. Você executa essa etapa de configuração usando o NetApp Console.

Saiba mais sobre os pools de recursos no Active IQ Unified Manager

Os pools de recursos são grupos de agregados criados por um administrador de storage usando o Unified Manager para fornecer provisionamento a aplicativos parceiros para gerenciamento de backups.

Você pode agrupar seus recursos com base em atributos como desempenho, custo, localização física ou disponibilidade. Ao agrupar recursos relacionados em um pool, você pode tratar o pool como uma única unidade para monitoramento e provisionamento. Isso simplifica o gerenciamento desses recursos e permite um uso mais flexível e eficiente do storage.

Durante o provisionamento de storage secundário, o Unified Manager determina o agregado mais adequado no pool de recursos para proteção usando os seguintes critérios:

- O agregado é um agregado de dados (não um agregado de raiz) e está ONLINE.
- O agregado está em um nó do cluster de destino cuja versão do ONTAP é igual ou superior à versão principal do cluster de origem.
- O agregado possui o maior espaço disponível dentre todos os agregados no pool de recursos.
- Após o provisionamento do volume de destino, o espaço do agregado está dentro do limite de quase cheio e quase supercomprometido definido para o agregado (limite global ou local, conforme aplicável).

- O número de volumes FlexVol no nó de destino não deve exceder o limite da plataforma.

Crie pools de recursos no Active IQ Unified Manager

Você pode usar a caixa de diálogo Criar pool de recursos para agrupar agregados para fins de provisionamento.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

Os pools de recursos podem conter agregados de diferentes clusters, mas o mesmo agregado não pode pertencer a diferentes pools de recursos.

1. No painel de navegação esquerdo, clique em **Proteção** > **Pools de recursos**.
2. Na página **Pool 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 no Active IQ Unified Manager

Você pode editar um pool de recursos existente quando quiser alterar o nome e a descrição do pool de recursos.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

O botão **Editar** só fica habilitado quando um pool de recursos é selecionado. Se mais de um pool de recursos for selecionado, o botão **Editar** fica 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 de pools de recursos.

Visualize o inventário do pool de recursos no Active IQ Unified Manager

Você pode usar a página Pools de recursos para visualizar o inventário de pools de recursos e monitorar a capacidade restante de cada pool de recursos.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Etapa

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 no Active IQ Unified Manager

Um pool de recursos consiste em vários agregados membros. Você pode adicionar agregados a pools de recursos existentes para aumentar a quantidade de espaço disponível para o provisionamento de volumes secundários.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Você pode adicionar no máximo 200 agregados a um pool de recursos por vez. Os agregados exibidos 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 da lista **Resource Pools**.

   Os membros do pool de recursos são exibidos na área abaixo da lista de pools 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 **Add**.

   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 em Active IQ Unified Manager

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 precisa ter a função de Application Administrator ou Storage Administrator.

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 os agregados membros.

   A lista de agregados de membros é exibida no painel Membros.

3. Selecione um ou mais agregados.

O botão **Remover** está ativado.

4. Clique em **Remover.**

   Uma caixa de diálogo de aviso é exibida.

5. Clique em **Yes** para continuar.

   Os agregados selecionados são removidos do painel Membros.

Excluir pools de recursos no Active IQ Unified Manager

Você pode excluir pools de recursos quando eles não forem mais necessários. Por exemplo, você pode querer redistribuir os agregados membro de um pool de recursos para vários outros pools de recursos, tornando obsoleto o pool de recursos original.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

O botão **Excluir** só fica habilitado 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 **Delete**.

   O pool de recursos é removido da lista de pools de recursos, e seus agregados são removidos da lista de membros.

Monitore as relações de proteção de recuperação de desastres da Storage VM

Saiba mais sobre as relações de recuperação de desastres de máquinas virtuais de armazenamento no Active IQ Unified Manager

O Active IQ Unified Manager oferece suporte ao monitoramento de relacionamentos de recuperação de desastres de VM de storage, o que fornece recuperação de desastres na granularidade do nível de uma VM de storage. A recuperação de desastres de VM de storage permite a recuperação dos dados presentes nos volumes constituintes da VM de storage, bem como a recuperação da configuração da VM de storage.

Uma relação de DR de VM de storage é criada da VM de storage de origem para a VM de storage de destino para fornecer recuperação de desastres assíncrona. Você pode optar por replicar toda a configuração da VM de storage ou um subconjunto dela (excluindo a configuração de rede e de protocolo), juntamente com os volumes de dados, com base na configuração do cluster.

Após a configuração da relação de recuperação de desastres da VM de storage, quando a VM de storage de origem fica indisponível devido a falha de hardware ou desastre ambiental, a VM de storage de destino é iniciada, fornecendo acesso aos dados com o mínimo de interrupção. Da mesma forma, quando a VM de storage de origem volta a ficar disponível, ela é ressincronizada com a VM de storage de destino e, em seguida, a origem é reiniciada para fornecer dados. Você pode usar os comandos do SnapMirror para configurar e gerenciar a relação de recuperação de desastres da VM de storage.

Monitore as VMs de armazenamento usando a página Relacionamentos no Active IQ Unified Manager

Você pode monitorar os relacionamentos de recuperação de desastres das suas VMs de armazenamento na página Relacionamentos, na seção PROTEÇÃO do INVENTÁRIO. Por padrão, a página Relacionamentos lista apenas os relacionamentos de nível superior, pois o filtro de relacionamentos constituintes está aplicado.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Você usa filtros para visualizar as relações de recuperação de desastres das VMs de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **PROTECTION** > **Relationships**.

   A página exibe todos os tipos de relacionamentos: volume, grupo de consistência e relacionamentos de máquina virtual de armazenamento.

2. Clique em **Filtrar** e, em seguida, selecione **Tipo de Objeto de Relacionamento** e **VM de Armazenamento** para visualizar apenas os relacionamentos de recuperação de desastres de VMs de armazenamento.
3. Clique em **Aplicar filtro**.

   Você deve limpar o filtro de relações de constituintes para visualizar todas as relações de proteção.

   A página exibe apenas os relacionamentos de recuperação de desastres das máquinas virtuais de armazenamento.

Visualize as relações de proteção da página de VMs de armazenamento em Active IQ Unified Manager

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 precisa ter a função de Application Administrator ou Storage Administrator.

Você também pode examinar detalhes das relações de proteção, incluindo o status da transferência e do atraso, além dos detalhes da origem e do destino. É possível agendar relatórios ou baixar relatórios existentes no formato desejado. O botão **Mostrar/Ocultar** permite adicionar as colunas necessárias aos relatórios, já que elas não são exibidas por padrão.

Passos

1. No painel de navegação esquerdo, clique em **STORAGE** > **Storage VMs**.
2. No menu **EXIBIR**, selecione **Relacionamento** > **Todos os Relacionamentos**.

   A visualização "Relacionamento: todos os Relacionamentos" exibe todas as VMs de armazenamento configuradas.

Visualize as VMs de armazenamento com base no status de proteção no Active IQ Unified Manager

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 precisa ter a função de Application Administrator ou Storage Administrator.

Uma nova coluna Função de proteção foi adicionada à visualização de VMs de armazenamento e 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 **STORAGE** > **Storage VMs**.
2. No menu **VISUALIZAR**, selecione **Saúde** > **Todas as VMs de armazenamento**.

   A "Saúde: todas as VMs de armazenamento" é exibida.

3. Clique em **Filtrar** 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 simultaneamente. Você precisará limpar o filtro existente para aplicar uma nova opção de filtro.

4. Clique em **Aplicar filtro**.

   A visualização "Unsaved" exibe todas as VMs de armazenamento que estão protegidas ou desprotegidas pela recuperação de desastres de VM de armazenamento, com base nas suas seleções de filtro.

Gerencie as associações de máquinas virtuais de armazenamento no Active IQ Unified Manager

As associações de máquinas virtuais de armazenamento (VMs de armazenamento) são mapeamentos de uma VM de armazenamento de origem para uma VM de armazenamento de destino, usados por aplicativos parceiros para a seleção de recursos e o provisionamento de volumes secundários.

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 secundário como origem para criar uma associação com uma VM de armazenamento de destino terciário.

Como administrador de aplicativos ou administrador de armazenamento, você pode visualizar as associações

de VMs de armazenamento em seu ambiente na página **Proteção** > **Associações de VMs 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 VMs de armazenamento de destino. Isso significa que todas as VMs de armazenamento existentes que atualmente precisam de proteção, bem como quaisquer VMs de armazenamento que forem criadas no futuro, serão associadas às VMs de armazenamento de destino especificadas. Por exemplo, você pode querer que aplicativos de várias origens diferentes em locais diferentes sejam copiados para uma ou mais VMs de armazenamento 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 VMs de armazenamento de destino específicas. Por exemplo, se você fornece serviços de armazenamento para muitos clientes cujos dados devem ser mantidos separados, pode escolher esta opção para associar uma VM de armazenamento de origem específica a uma VM de armazenamento de destino específica atribuída somente a esse cliente.
- **Associar a uma VM de armazenamento externa**: 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 máquinas virtuais de armazenamento permite que os aplicativos de proteção de parceiros associem uma VM de armazenamento de origem a uma VM de armazenamento de destino para uso com o SnapMirror e o SnapVault. Os aplicativos de parceiros usam essas associações no momento do provisionamento inicial de volumes de destino para determinar quais recursos selecionar.dd

Antes de começar

- A máquina virtual de armazenamento que você está associando já deve existir.
- Você precisa ter a função de Application Administrator ou Storage Administrator.

Para qualquer máquina virtual de armazenamento de origem e tipo de relacionamento, você pode escolher apenas uma máquina virtual de armazenamento de destino em cada cluster de destino.

Alterar associações usando as funções de exclusão e criação afeta apenas as operações futuras de provisionamento. Isso não move os volumes de destino existentes.

Passos

1. No painel de navegação esquerdo, clique em **Proteção** > **Associações de VMs de armazenamento**.
2. Na página **Associações de VMs de armazenamento**, clique em **Criar**.

   O assistente **Criar associações de máquinas virtuais de armazenamento** é aberto.

3. Selecione uma das seguintes origens:
   - **Qualquer**

     Escolha esta opção quando você quiser criar uma associação entre qualquer VM de storage de origem do storage primário e uma ou mais VMs de storage de destino. Isso significa que todas as VMs de storage existentes que atualmente exigem proteção, bem como quaisquer VMs de storage criadas no futuro, serão associadas à VM de storage de destino especificada. Por exemplo, você pode querer que aplicativos de várias origens diferentes em locais distintos tenham backup em uma ou mais VMs de storage de destino em um único local.

- **Único**

  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 vários clientes cujos dados devem ser mantidos separados entre si, escolha esta opção para associar uma VM de armazenamento de origem específica a uma VM de armazenamento de destino atribuída somente a esse cliente.

- **Nenhum (Externo)**

  Escolha esta opção quando quiser criar uma associação entre uma máquina virtual de armazenamento de origem e um volume flexível externo de uma máquina virtual de armazenamento de destino.

4. Selecione um ou ambos os tipos de relação de proteção que você deseja criar:
   - **O SnapMirror**
   - **o SnapVault**
5. Clique em **Avançar**.
6. Selecione um ou mais destinos de proteção da VM de storage.
7. Clique em **Concluir**.

Excluir associações de VM de storage

Você pode excluir associações de VM de storage para aplicativos parceiros a fim de remover a relação de provisionamento secundário entre a VM de storage de origem e a de destino; por exemplo, você pode fazer isso quando a VM de storage de destino estiver cheia e quiser criar uma nova associação de proteção de VM de storage.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

O botão **Excluir** fica desativado até que pelo menos uma associação de VM de storage seja selecionada. Alterar associações usando as funções de exclusão e criação afeta apenas as operações futuras de provisionamento; não move os volumes de destino existentes.

Passos

1. No painel de navegação esquerdo, clique em **Proteção** > **Associações de VMs de armazenamento**.
2. Selecione pelo menos uma associação da VM de storage.

   O botão **Excluir** está habilitado.

3. Clique em **Excluir.**

   Uma caixa de diálogo de aviso é exibida.

4. Clique em **Yes** para continuar.

   A associação de máquina virtual de armazenamento selecionada foi removida da lista.

Requisitos de SVM e de pool de recursos para suportar serviços de storage no Active IQ Unified Manager

Você pode garantir melhor a conformidade em aplicativos parceiros se observar alguns requisitos de associação de SVM e de pool de recursos específicos para serviços de storage: por exemplo, ao associar a SVM e criar pools de recursos no Unified Manager para dar suporte a uma topologia de proteção em um serviço de storage fornecido por um aplicativo parceiro.

Algumas aplicações fazem parceria com o servidor do Unified Manager para fornecer serviços que configuram e executam automaticamente a proteção de backup do SnapMirror ou do SnapVault entre volumes de origem e volumes de proteção em locais secundários ou terciários. Para dar suporte a esses serviços de storage de proteção, você deve usar o Unified Manager para configurar as associações de SVM e os pools de recursos necessários.

Para oferecer suporte à proteção de serviço de storage de salto único ou em cascata, incluindo a replicação de uma fonte do SnapMirror ou de um volume primário do SnapVault para o destino do SnapMirror 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 a SVM que contém o volume de origem do SnapMirror ou o volume primário do SnapVault e qualquer SVM na qual resida um volume secundário ou um volume terciário.
  - Por exemplo, para oferecer suporte a uma topologia de proteção em que o volume de origem Vol_A reside em SVM_1, e 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 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 do SnapMirror ou associação de backup do SnapVault entre SVM_2 e SVM_3 não é necessária e não é usada.

  - Para suportar uma topologia de proteção em que tanto o volume de origem Vol_A quanto o volume de destino do SnapMirror Vol_B residem em SVM_1, você deve configurar uma associação do SnapMirror entre SVM_1 e SVM_1.
- Os pools de recursos devem incluir recursos de agregados de cluster disponíveis para as SVMs associadas.

  Você configura os 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 storage.

Saiba mais sobre os jobs no Active IQ Unified Manager

Um trabalho é uma série de tarefas que você pode monitorar usando o Unified Manager. Visualizar os trabalhos e suas respectivas tarefas permite que você determine se foram concluídos com sucesso.

Os trabalhos são iniciados quando você cria relacionamentos de SnapMirror e SnapVault, quando realiza qualquer operação de relacionamento (quebrar, editar, suspender, remover, retomar, ressincronizar e reverter a ressincronização), quando executa tarefas de restauração de dados, quando faz login em um cluster e assim por diante.

Quando você inicia um trabalho, pode usar a página Trabalhos e a página Detalhes do trabalho para monitorar o trabalho e o progresso das tarefas de trabalho associadas.

Monitore tarefas no Active IQ Unified Manager

Você pode usar a página Jobs para monitorar o status da tarefa e visualizar propriedades da tarefa, como tipo de serviço de armazenamento, estado, horário de envio e horário de conclusão, para determinar se uma tarefa foi concluída com sucesso.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Proteção** > **Tarefas**.

   A página Jobs é exibida.

2. Consulte a coluna **Estado** para determinar o status dos trabalhos em execução no momento.
3. Clique no nome de uma tarefa para ver detalhes sobre essa tarefa específica.

   A página de detalhes do trabalho é exibida.

Veja os detalhes do trabalho no Active IQ Unified Manager

Após iniciar um trabalho, você pode acompanhar seu progresso na página de detalhes do trabalho e monitorar as tarefas associadas para detectar possíveis erros.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Proteção** > **Tarefas**.
2. Na página Trabalhos, clique no nome de um trabalho na coluna **Nome** para exibir a lista de tarefas associadas ao trabalho.
3. Clique em uma tarefa para exibir informações adicionais no painel **Detalhes da Tarefa** e no painel **Mensagens da Tarefa** à direita da lista de tarefas.

Cancelar tarefas no Active IQ Unified Manager

Você pode usar a página Jobs para abortar um trabalho se ele estiver demorando muito para terminar, estiver encontrando muitos erros ou não for mais necessário. Você só pode abortar um trabalho se o status e o tipo dele permitirem. Você pode abortar qualquer trabalho em execução.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Proteção** > **Tarefas**.

2. Na lista de trabalhos, selecione um trabalho e clique em **Abort**.
3. No prompt de confirmação, clique em **Yes** para abortar a tarefa selecionada.

Tente novamente uma tarefa de proteção com falha no Active IQ Unified Manager

Após tomar medidas para corrigir uma tarefa de proteção com falha, você pode usar **Tentar novamente** para executar a tarefa novamente. Tentar novamente uma tarefa cria uma nova tarefa usando o ID da tarefa original.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Você só pode tentar novamente uma tarefa com falha por vez. Selecionar mais de uma tarefa desativa o botão **Tentar novamente**. Somente tarefas do tipo Configuração de Proteção e Operação de Relacionamento de Proteção podem ser tentadas novamente.

Passos

1. No painel de navegação esquerdo, clique em **Proteção** > **Tarefas**.
2. Na lista de tarefas, selecione uma única tarefa com falha do tipo Configuração de Proteção ou Operação de Relação de Proteção.

   O botão **Tentar novamente** está ativado.

3. Clique em **Tentar novamente**.

   A tarefa foi reiniciada.

Descrição das janelas e caixas de diálogo de relacionamentos de proteção

Saiba mais sobre a página de pools de recursos no Active IQ Unified Manager

A página "Resource Pools" exibe os 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**

  Abre 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 excluir um ou mais pools de recursos.

Lista de pools de recursos

A lista de 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.

- **SnapLock Tipo**

  Exibe o tipo SnapLock que está sendo usado pelos agregados no pool de recursos. Os valores válidos para o tipo SnapLock são Compliance, Enterprise e Non-SnapLock. Um pool de recursos pode conter agregados de apenas um tipo SnapLock.

- **Capacidade Total**

  Exibe a capacidade total (em MB, GB e assim por diante) do pool de recursos.

- **Capacidade Utilizada**

  Exibe a quantidade de espaço (em MB, GB etc.) que é usada no pool de recursos.

- **Capacidade disponível**

  Exibe a quantidade de espaço (em MB, GB, etc.) disponível no pool de recursos.

- **% usado**

  Exibe a porcentagem de espaço que está sendo usado 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 Membros exibe (em formato tabular) os membros do pool de recursos e suas propriedades quando um pool de recursos é selecionado.

- **Status**

  Exibe o status atual do agregado membro. O status pode ser Crítico (), Erro (), Aviso () ou Normal ().

- **Nome do agregado**

  Exibe o nome do agregado membro.

- **Estado**

  Exibe o estado atual do agregado, que pode ser um dos seguintes:

  - Offline

    O acesso de leitura/gravação não é permitido.

  - Online

    O acesso de leitura/gravação aos volumes hospedados neste agregado é permitido.

  - Restrito

    Operações limitadas (como reconstrução de paridade) são permitidas, mas o acesso aos dados não é permitido.

  - Criando

    O agregado está sendo criado.

  - Destruindo

    O agregado está sendo destruído.

  - Falha

    O agregado não pode ser colocado online.

  - Congelado

    O agregado não está (temporariamente) atendendo solicitações.

  - Inconsistente

    O agregado foi marcado como corrompido; entre em contato com o suporte técnico.

  - Ferro restrito

    Não é possível executar ferramentas de diagnóstico no agregado.

  - Montagem

    O agregado está em processo de montagem.

  - Parcial

    Pelo menos um disco foi encontrado para o agregado, mas faltam dois ou mais discos.

  - Colocando em quiescência

    O agregado está sendo colocado em quiescência.

- Em estado inativo

  O agregado está em quiescência.

- Revertido

  A reversão de um agregado foi concluída.

- Desmontado

  O agregado foi desmontado.

- Desmontagem

  O agregado está sendo colocado offline.

- Desconhecido

  O agregado foi descoberto, mas as informações do agregado ainda não foram recuperadas pelo servidor do Unified Manager.

Por padrão, esta coluna está oculta.

- **Cluster**

  Exibe o nome do cluster ao qual o agregado pertence.

- **Nó**

  Exibe o nome do nó no qual o agregado está localizado.

- **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) usada no agregado.

- **Capacidade disponível**

  Exibe a quantidade de espaço (em MB, GB etc.) disponível no agregado.

- **% usado**

  Exibe a porcentagem de espaço utilizado 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.

Utilize a caixa de diálogo Criar pool de recursos no Active IQ Unified Manager

Você pode usar a caixa de diálogo Criar Conjunto de Recursos para nomear e descrever um novo pool de recursos, bem como para adicionar agregados a esse pool de recursos e excluir agregados dele.

Nome do pool de recursos

As caixas de texto permitem adicionar as seguintes informações para criar um pool de recursos:

Permite especificar um nome para o 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 "Aggregates" para que você possa adicionar agregados de um cluster específico ao pool de recursos. Você pode adicionar agregados de clusters diferentes, mas os mesmos agregados não podem ser adicionados a mais de um pool de recursos.

- **Remover**

  Permite remover agregados selecionados do pool de recursos.

- **Criar**

  Cria o pool de recursos. Este botão só será habilitado depois que informações forem inseridas nos campos Nome do pool de recursos ou Descrição.

- **Cancelar**

  Descarta as alterações e fecha a caixa de diálogo Create Resource Pool.

Utilize a caixa de diálogo Editar pool de recursos no Active IQ Unified Manager

Você pode usar a caixa de diálogo Edit Resource Pool 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 inserir 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.

Utilize a caixa de diálogo de agregações no Active IQ Unified Manager

Você pode usar a caixa de diálogo Aggregates 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 só fica habilitado depois que pelo menos um agregado for selecionado.

- **Cancelar**

  Descarta as alterações e fecha a caixa de diálogo Aggregates.

Lista de agregados

A lista de agregados exibe (em formato tabular) os nomes e as 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:

  - Offline

    O acesso de leitura/gravação não é permitido.

  - Restrito

    Operações limitadas (como reconstrução de paridade) são permitidas, mas o acesso aos dados não é permitido.

  - Online

    O acesso de leitura/gravação aos volumes hospedados neste agregado é permitido.

  - Criando

    O agregado está sendo criado.

  - Destruindo

    O agregado está sendo destruído.

  - Falha

    O agregado não pode ser colocado online.

  - Congelado

    O agregado não está (temporariamente) atendendo solicitações.

  - Inconsistente

    O agregado foi marcado como corrompido; entre em contato com o suporte técnico.

  - Ferro restrito

    Não é possível executar ferramentas de diagnóstico no agregado.

  - Montagem

    O agregado está em processo de montagem.

  - Parcial

    Pelo menos um disco foi encontrado para o agregado, mas faltam dois ou mais discos.

  - Colocando em quiescência

    O agregado está sendo colocado em quiescência.

  - Em estado inativo

    O agregado está em quiescência.

- Revertido

  A reversão de um agregado foi concluída.

- Desmontado

  O agregado está offline.

- Desmontagem

  O agregado está sendo colocado offline.

- Desconhecido

  O agregado foi descoberto, mas as informações do agregado ainda não foram recuperadas pelo servidor do Unified Manager.

- **Cluster**

  Exibe o nome do cluster no qual o agregado está localizado.

- **Nó**

  Exibe o nome do controlador de armazenamento que contém o agregado.

- **Capacidade Total**

  Exibe o tamanho total dos dados (em MB, GB etc.) do agregado. Por padrão, esta coluna fica oculta.

- **Capacidade Comprometida**

  Exibe o espaço total (em MB, GB etc.) alocado para todos os volumes no agregado. Por padrão, esta coluna fica oculta.

- **Capacidade Utilizada**

  Exibe a quantidade de espaço (em MB, GB e assim por diante) usada no agregado.

- **Capacidade disponível**

  Exibe a quantidade de espaço (em MB, GB, etc.) disponível para os dados no agregado. Por padrão, esta coluna fica 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 de RAID**

  Exibe o tipo de RAID do volume selecionado. O tipo de RAID pode ser RAID0, RAID4, RAID-DP, RAID-TEC ou RAID misto.

Saiba mais sobre a página de jobs no Active IQ Unified Manager

A página Jobs permite que você veja o status atual e outras informações sobre todos os trabalhos de proteção de aplicativos parceiros que estão em execução no momento, bem como os trabalhos que já foram concluídos. Você pode usar essas informações para ver quais trabalhos ainda estão em execução e se um trabalho foi concluído com sucesso ou falhou.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Abortar**

  Cancela a tarefa selecionada. Esta opção só está disponível se a tarefa selecionada estiver em execução.

- **Tentar novamente**

  Reinicia uma tarefa 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 **Tentar novamente** ficará desabilitado. Não é possível tentar novamente tarefas com falha do serviço de armazenamento.

- **Atualizar**

  Atualiza a lista de jobs e as informações associadas a eles.

Lista de trabalhos

A lista de trabalhos exibe, em formato tabular, uma lista dos trabalhos em andamento. Por padrão, a lista exibe apenas os trabalhos gerados na última semana. Você pode usar a classificação por colunas e a filtragem 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 da tarefa. Por padrão, esta coluna está oculta.

  O número de identificação da tarefa é único e é atribuído pelo servidor quando a tarefa é iniciada. Você pode pesquisar uma tarefa específica inserindo o número de identificação da tarefa 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**

Uma tarefa do Workflow Automation está redescobrindo um cluster.

- **Configuração de proteção**

  Uma tarefa de proteção inicia fluxos de trabalho do Workflow Automation, como agendamentos cron, criação de políticas do SnapMirror e assim por diante.

- **Operação de Relação de Proteção**

  Um trabalho de proteção está executando operações do SnapMirror.

- **Cadeia de Fluxo de Trabalho de Proteção**

  Uma tarefa do Workflow Automation executa vários fluxos de trabalho.

- **Restaurar**

  Uma tarefa de restauração está em execução.

- **Limpar**

  A tarefa consiste em limpar os artefatos dos membros do serviço de armazenamento que não são mais necessários para fins de restauração.

- **Conformidade**

  A tarefa consiste em verificar a configuração dos membros do serviço de armazenamento para garantir que estejam em conformidade.

- **Destruir**

  A tarefa está excluindo um serviço de armazenamento.

- **Importar**

  A tarefa consiste em importar objetos de armazenamento não gerenciados para um serviço de armazenamento existente.

- **Modificar**

  A tarefa consiste em modificar os atributos de um serviço de armazenamento existente.

- **Inscreva-se**

  A tarefa consiste em inscrever membros em um serviço de armazenamento.

- **Cancelar inscrição**

  A tarefa consiste em cancelar a assinatura de membros de um serviço de armazenamento.

- **Atualizar**

  Uma tarefa de atualização de proteção está em execução.

- **Configuração do WFA**

Uma tarefa do Workflow Automation está enviando credenciais do cluster e sincronizando caches do banco de dados.

- **Estado**

  Exibe o estado de execução da tarefa. As opções de estado são as seguintes:

  - **Abortado**

    A tarefa foi abortada.

  - **Abortando**

    A tarefa está em processo de cancelamento.

  - **Concluído**

    O trabalho está concluído.

  - **Em execução**

    A tarefa está em execução.

- **Hora de envio**

  Exibe a hora em que o trabalho foi submetido.

- **Duração**

  Exibe o tempo que a tarefa levou para ser concluída. Esta coluna é exibida por padrão.

- **Tempo de conclusão**

  Exibe a hora em que a tarefa foi concluída. Por padrão, esta coluna está oculta.

Saiba mais sobre a página de detalhes do trabalho no Active IQ Unified Manager

A página de detalhes da tarefa permite que você visualize o status e outras informações sobre tarefas específicas de proteção que estão em execução, na fila ou que foram concluídas. Você pode usar essas informações para monitorar o progresso das tarefas de proteção e solucionar problemas relacionados a falhas.

Resumo do trabalho

O resumo do trabalho exibe as seguintes informações:

- ID do trabalho
- Tipo
- Estado
- Hora de envio
- Tempo de conclusão
- 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 tarefas**

  Leva você de volta à página Jobs.

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 foi iniciada. Por padrão, as tarefas mais recentes são exibidas na parte superior da coluna e as tarefas mais antigas são exibidas na parte inferior.

- **Tipo**

  Exibe o tipo de tarefa.

- **Estado**

  O estado de uma tarefa específica:

  - **Concluído**

    A tarefa está concluída.

  - **Na fila**

    A tarefa está prestes a ser executada.

  - **Em execução**

    A tarefa está em execução.

  - **Aguardando**

    Um trabalho foi enviado, e algumas tarefas associadas aguardam entrada na fila e execução.

- **Status**

  Exibe o status da tarefa:

  - **Erro (❗)**

    A tarefa falhou.

  - **Normal (✅)**

    A tarefa foi concluída com sucesso.

- **Ignorado ( )**

  Uma tarefa falhou, fazendo com que as tarefas subsequentes fossem ignoradas.

- **Duração**

  Exibe o tempo decorrido desde o início da tarefa.

- **Tempo de conclusão**

  Exibe a hora em que a tarefa foi concluída. Por padrão, esta coluna fica oculta.

- **ID da tarefa**

  Exibe o GUID que identifica uma tarefa individual de um trabalho. A coluna pode ser classificada e filtrada. Por padrão, esta coluna está oculta.

- **Ordem de dependência**

  Exibe um número inteiro que representa a sequência de tarefas em um gráfico, sendo zero 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, caso a tarefa tenha falhado, o motivo da falha.

- **Painel de mensagens da tarefa**

  Exibe mensagens específicas da tarefa selecionada. As mensagens podem incluir o motivo do erro e sugestões para resolvê-lo. Nem todas as tarefas exibem mensagens da tarefa.

Utilize a caixa de diálogo Configurações Secundárias Avançadas no Active IQ Unified Manager

Você pode usar a caixa de diálogo Configurações Secundárias Avançadas para habilitar a replicação flexível por versão, o backup de múltiplas cópias e as 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: deduplicação, compressão de dados, crescimento automático e garantia de espaço.

A caixa de diálogo inclui os seguintes campos:

- **Habilitar replicação flexível por versão**

  Habilita o SnapMirror com replicação flexível em termos de versão. A replicação flexível em termos de versão permite a proteção do SnapMirror de um volume de origem, mesmo que o volume de destino esteja executando uma versão anterior do ONTAP em relação à do volume de origem.

  - Ativar backup

    Se a replicação flexível por versão estiver ativada, também permite que várias cópias de Snapshot dos

dados de origem do SnapMirror sejam transferidas e mantidas no destino do SnapMirror.

- **Ativar a desduplicação**

  Habilita a deduplicação no volume secundário em uma relação do SnapVault, para que blocos de dados duplicados sejam eliminados e você economize espaço. Você pode usar a deduplicação quando a economia de espaço for de pelo menos 10% e a taxa de substituição de dados não for alta. A deduplicação é frequentemente usada em ambientes virtualizados, compartilhamentos de arquivos e dados de backup. Essa configuração fica desativada por padrão. Quando habilitada, essa operação é iniciada após cada transferência.

  - Ativar compressão

    Habilita a compressão de dados transparente. Você pode usar a compressão 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 compressão seja concluída fora dos horários de pico. Em uma relação do SnapVault, essa configuração é desativada por padrão. A compressão está disponível somente quando a desduplicação é selecionada.

  - Comprimir em linha

    Permite economia imediata de espaço ao compactar os dados antes de gravá-los no disco. Você pode usar a compactação em linha quando o sistema não tiver mais de 50 por cento de utilização durante os horários de pico e quando o sistema puder acomodar novas gravações e CPU adicional durante os horários de pico. Essa configuração está disponível somente quando “Enable Compression” estiver selecionado.

- **Ativar o Autogrow**

  Permite aumentar 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 só é habilitado quando a configuração de crescimento automático está ativada.

- **Tamanho do incremento**

  Especifica o incremento percentual pelo qual o volume cresce automaticamente antes de atingir a porcentagem máxima do volume de origem.

- **Garantia de espaço**

  Garante que haja espaço suficiente alocado no volume secundário para que as transferências de dados sejam sempre bem-sucedidas. A configuração da garantia de espaço pode ser uma das seguintes:

  - Arquivo
  - Volume
  - None + Por exemplo, você pode ter um volume de 200 GB que contém arquivos totalizando 50 GB; no entanto, esses arquivos contêm apenas 10 GB de dados. A garantia de volume aloca 200 GB para o volume de destino, independentemente do conteúdo na origem. A garantia de arquivo aloca 50 GB

para garantir que haja espaço suficiente reservado para os arquivos na origem; selecionar None nesse cenário significa que apenas 10 GB serão alocados no destino para o espaço realmente usado pelos dados dos arquivos na origem.

A garantia de espaço está 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 **Apply** na caixa de diálogo Configure Protection.

- **Cancelar**

  Descarta suas seleções e fecha a caixa de diálogo Advanced Destination Settings.

Utilize a caixa de diálogo Configurações Avançadas de Destino no Active IQ Unified Manager

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 as configurações avançadas quando a garantia de espaço estiver desabilitada na origem, mas quiser habilitá-la no destino. As configurações de deduplicação, compactação e crescimento automático em uma relação do SnapMirror são herdadas do volume de origem e não podem ser alteradas.

Garantia de espaço

Garante que haja espaço suficiente alocado no volume de destino para que as transferências de dados sejam sempre bem-sucedidas. A configuração de garantia de espaço pode ser uma das seguintes:

- 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 para o volume de destino, independentemente do conteúdo na origem. A garantia de arquivo aloca 50 GB para garantir que haja espaço suficiente reservado para os arquivos de origem no destino; selecionar **None** nesse cenário significa que apenas 10 GB são alocados no destino para o espaço realmente usado pelos dados dos arquivos na origem.

A garantia de espaço está definida como Volume por padrão.

Utilize a caixa de diálogo Restaurar no Active IQ Unified Manager

Você pode usar a caixa de diálogo Restaurar para restaurar dados em um volume a partir de uma cópia Snapshot específica.

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 Snapshot**

  Especifica qual cópia Snapshot você deseja usar para restaurar os dados. Por padrão, a cópia Snapshot mais recente é selecionada. Você também pode selecionar uma cópia Snapshot diferente na lista suspensa. A lista de cópias Snapshot muda de acordo com o volume selecionado.

- **Liste no máximo 995 arquivos e diretórios**

  Por padrão, a lista mostra no máximo 995 objetos. Você pode desmarcar esta caixa de seleção se quiser visualizar todos os objetos no volume selecionado. Esta operação pode demorar um pouco se o número de itens for muito grande.

Selecione os itens que deseja 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 ficam 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. Clicar em  após escolher um caminho faz você subir um nível na estrutura de diretórios.

- **Lista de pastas e arquivos**

  Exibe o conteúdo do caminho que você inseriu. Por padrão, a pasta raiz é exibida inicialmente. Clicar no nome de uma pasta exibe o conteúdo dela.

Você pode selecionar os itens a serem restaurados da seguinte forma:

- Ao inserir o caminho com um nome de arquivo específico no campo de caminho, o arquivo especificado é exibido em Folders and Files.
- Ao inserir um caminho sem especificar um arquivo em particular, o conteúdo da pasta é exibido na lista de 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 itens demais para serem mostrados, e se você prosseguir com a operação, todos os itens da pasta especificada serão restaurados. Você pode desmarcar a caixa de seleção “List maximum of 995 files and directories” se quiser visualizar todos os objetos no 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 do qual foi feito backup dos dados originalmente.

- **Localização alternativa**

  Restaura os dados selecionados em 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 a hierarquia de diretórios

    Quando selecionada, essa opção 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 diretórios 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 as suas seleções e fecha a caixa de diálogo Restaurar.

- **Restaurar**

  Aplica suas seleções e inicia o processo de restauração.

Utilize a caixa de diálogo Procurar diretórios no Active IQ Unified Manager

Você pode usar a caixa de diálogo Procurar Diretórios quando quiser restaurar dados para um diretório em um cluster e SVM diferente da origem original. O cluster de origem e o volume de origem originais são selecionados por padrão.

A caixa de diálogo Procurar diretórios permite selecionar o cluster, SVM, volume e caminho do diretório para o qual você deseja restaurar os dados.

- **Cluster**

  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 de SVM**

  Lista as SVMs disponíveis para o cluster selecionado. Por padrão, a SVM do volume de origem original é selecionada.

- **Volume**

  Lista todos os volumes de leitura/gravação em uma SVM selecionada. 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 de origem original é selecionado.

- **Caixa de texto com o caminho do arquivo**

  Permite que você digite o caminho do arquivo para o qual deseja restaurar os dados. O caminho inserido deve já existir.

- **Nome**

  Exibe os nomes das pastas disponíveis no volume selecionado. Clicar em uma pasta na lista Nome exibe as subpastas, se houver. Os arquivos contidos nas pastas não são exibidos. Clicar em  após selecionar uma pasta move você um nível acima na estrutura de diretórios.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Selecionar diretório**

  Aplica suas seleções e fecha a caixa de diálogo Procurar diretórios. Se nenhum diretório estiver selecionado, este botão fica desativado.

- **Cancelar**

  Descarta suas seleções e fecha a caixa de diálogo Browse Directories.

Utilize a caixa de diálogo Configurar Proteção no Active IQ Unified Manager

Você pode usar a caixa de diálogo Configurar proteção para criar relações do SnapMirror e do SnapVault para todos os volumes de leitura, gravação e proteção de dados nos clusters, para garantir que os dados em um volume de origem ou volume primário sejam replicados.

Guia Origem

- **Vista de topologia**

  Exibe uma representação visual da relação que você está criando. A origem na topologia é destacada por padrão.

- **Informações de origem**

  Exibe detalhes sobre os volumes de origem selecionados, incluindo as seguintes informações:

  - Nome do cluster de origem
  - Nome da SVM de origem
  - Tamanho total cumulativo do volume

    Exibe o tamanho total de todos os volumes de origem selecionados.

◦ Tamanho cumulativo usado do volume

Exibe o tamanho cumulativo usado do volume 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.

▪ SnapLock Tipo

Exibe o tipo de SnapLock do volume. As opções são Compliance, Enterprise e não SnapLock.

▪ Cópia Snapshot

Exibe a cópia Snapshot usada para a transferência completa. Se o volume de origem for leitura/gravação, o valor "Default" na coluna cópia Snapshot indica que uma nova cópia Snapshot é criada por padrão e usada para a transferência completa. Se o volume de origem for um volume de proteção de dados, o valor "Default" na coluna cópia Snapshot indica que nenhuma nova cópia Snapshot é criada, e todas as cópias Snapshot existentes são transferidas para o destino. Clicar no valor da cópia Snapshot exibe uma lista de cópias Snapshot, na qual você pode selecionar uma cópia Snapshot existente para usar na transferência completa. Você não pode selecionar uma cópia Snapshot padrão diferente se o tipo de origem for proteção de dados.

SnapMirror guia

Permite especificar um cluster de destino, uma máquina virtual de storage (SVM) e um agregado para uma relação de proteção, bem como uma convenção de nomenclatura para destinos ao criar uma relação do SnapMirror. Você também pode especificar uma política do SnapMirror e um agendamento.

- **Vista de topologia**

  Exibe uma representação visual da relação que você está criando. O recurso de destino do SnapMirror na topologia é destacado por padrão.

- **Informações sobre o destino**

  Permite selecionar os recursos de destino para uma relação de proteção:

  ◦ Link avançado

  Abre a caixa de diálogo Configurações avançadas de destino ao criar uma relação do SnapMirror.

  ◦ Cluster

  Lista os clusters que estão disponíveis como hosts de destino de proteção. Este campo é obrigatório.

  ◦ máquina virtual de storage (SVM)

Lista as SVMs disponíveis no cluster selecionado. É necessário selecionar um cluster para que a lista de SVMs seja exibida. Este campo é obrigatório.

◦ Agregado

Lista os agregados disponíveis no SVM selecionado. Um cluster deve ser selecionado antes que a lista de agregados seja preenchida. Este campo é obrigatório. A lista de agregados exibe as seguintes informações:

▪ Classificação

Quando vários agregados satisfazem todos os requisitos para um destino, a classificação indica a prioridade na qual o agregado é listado, de acordo com as seguintes condições:

A. É preferível que o agregado esteja localizado em um nó diferente do nó do volume de origem para permitir a separação do domínio de falhas.
B. É preferível um agregado em um nó com menos volumes para permitir o balanceamento de carga entre os nós de um cluster.
C. Para permitir o balanceamento de capacidade, é preferível um agregado que tenha mais espaço livre do que outros agregados. Uma classificação de 1 significa que o agregado é o mais preferido de acordo com os três critérios.

▪ Nome agregado

Nome do agregado

▪ Capacidade disponível
▪ Quantidade de espaço disponível no agregado para dados
▪ Pool de recursos

Nome do pool de recursos ao qual o agregado pertence

◦ Convenção de nomenclatura

Especifica a convenção de nomenclatura padrão aplicada ao volume de destino. Você pode aceitar a convenção de nomenclatura fornecida ou criar uma personalizada. A convenção de nomenclatura pode ter os seguintes atributos: %C, %M, %V e %N, em que %C é o nome do cluster, %M é o nome da SVM, %V é o volume de origem e %N é o nome do nó de destino da topologia.

O campo de convenção de nomenclatura é destacado em vermelho se a sua entrada for inválida. Clicar no link “Preview Name” exibe uma prévia da convenção de nomenclatura que você inseriu, e o texto da prévia é atualizado dinamicamente conforme você digita uma convenção de nomenclatura no campo de texto. Um sufixo entre 001 e 999 é acrescentado ao nome de destino quando a relação é criada, substituindo o nnn exibido no texto de prévia, com 001 sendo atribuído primeiro, 002 sendo atribuído em segundo lugar e assim por diante.

- **Configurações de relacionamento**

Permite especificar a taxa de transferência máxima, a política do SnapMirror e o cronograma que a relação de proteção utiliza:

◦ 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 máxima de transferência, a transferência completa entre relações será ilimitada.

- Política do SnapMirror

  Especifica a política do SnapMirror do ONTAP para a relação. O padrão é DPDefault.

- Criar política

  Abre a caixa de diálogo Criar política do SnapMirror, que permite criar e usar uma nova política do SnapMirror.

- SnapMirror Agendamento

  Especifica a política do ONTAP SnapMirror para a relação. Os agendamentos disponíveis incluem None, 5min, 8hour, daily, hourly e weekly. O padrão é None, indicando que nenhum agendamento está associado à relação. Relações sem agendamentos não têm valores de status de atraso, a menos que pertençam a um serviço de armazenamento.

- Criar programação

  Abre a caixa de diálogo Criar Agendamento, que permite criar um novo agendamento do SnapMirror.

SnapVault guia

Permite especificar um cluster secundário, SVM e agregado para uma relação de proteção, bem como uma convenção de nomenclatura para volumes secundários ao criar uma relação do SnapVault. Você também pode especificar uma política do SnapVault e um agendamento.

- **Vista de topologia**

  Exibe uma representação visual da relação que você está criando. O recurso secundário do SnapVault na topologia é destacado por padrão.

- **Informações secundárias**

  Permite selecionar os recursos secundários para uma relação de proteção:

  - Link avançado

    Abre a caixa de diálogo Configurações Secundárias Avançadas.

  - Cluster

    Lista os clusters disponíveis como hosts de proteção secundária. Este campo é obrigatório.

  - máquina virtual de storage (SVM)

    Lista as SVMs disponíveis no cluster selecionado. É necessário selecionar um cluster para que a lista de SVMs seja exibida. Este campo é obrigatório.

  - Agregado

    Lista os agregados disponíveis no SVM selecionado. Um cluster deve ser selecionado antes que a lista de agregados seja preenchida. Este campo é obrigatório. A lista de agregados exibe as seguintes informações:

- Classificação

  Quando vários agregados satisfazem todos os requisitos para um destino, a classificação indica a prioridade na qual o agregado é listado, de acordo com as seguintes condições:

  A. É preferível que o agregado esteja localizado em um nó diferente do nó do volume primário para permitir a separação do domínio de falhas.
  B. É preferível um agregado em um nó com menos volumes para permitir o balanceamento de carga entre os nós de um cluster.
  C. Para permitir o balanceamento de capacidade, é preferível um agregado que tenha mais espaço livre do que outros agregados. Uma classificação de 1 significa que o agregado é o mais preferido de acordo com os três critérios.

- Nome agregado

  Nome do agregado

- Capacidade disponível
- Quantidade de espaço disponível no agregado para dados
- Pool de recursos

  Nome do pool de recursos ao qual o agregado pertence

◦ Convenção de nomenclatura

  Especifica a convenção de nomenclatura padrão aplicada ao volume secundário. Você pode aceitar a convenção de nomenclatura fornecida ou criar uma personalizada. A convenção de nomenclatura pode ter os seguintes atributos: %C, %M, %V e %N, onde %C é o nome do cluster, %M é o nome da SVM, %V é o volume de origem e %N é o nome do nó secundário da topologia.

O campo de convenção de nomenclatura é destacado em vermelho se a sua entrada for inválida. Clicar no link “Preview Name” exibe uma pré-visualização da convenção de nomenclatura que você inseriu, e o texto da pré-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 pré-visualização. Um sufixo entre 001 e 999 é adicionado ao nome secundário quando a relação é criada, substituindo o nnn exibido no texto da pré-visualização, sendo 001 atribuído primeiro, 002 atribuído em segundo lugar e assim por diante.

- **Configurações de relacionamento**

  Permite especificar a taxa máxima de transferência, a política do SnapVault e a programação do SnapVault que a relação de proteção utiliza:

  ◦ 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 máxima de transferência, a transferência completa entre relações será ilimitada.

  ◦ SnapVault Política

    Especifica a política SnapVault do ONTAP para a relação. O padrão é XDPDefault.

  ◦ Criar política

Abre a caixa de diálogo Criar Política do SnapVault, que permite criar e usar uma nova política do SnapVault.

- SnapVault Agendamento

  Especifica o agendamento do SnapVault do ONTAP para a relação. Os agendamentos disponíveis incluem None, 5min, 8hour, daily, hourly e weekly. O padrão é None, indicando que nenhum agendamento está associado à relação. Relações sem agendamentos não têm valores de status de atraso, a menos que pertençam a um serviço de armazenamento.

- Criar programação

  Abre 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 Configure Protection.

- **Aplicar**

  Aplica suas seleções e inicia o processo de proteção.

Utilize a caixa de diálogo Criar Agendamento no Active IQ Unified Manager

A caixa de diálogo Criar Agendamento permite criar um agendamento de proteção básico ou avançado para transferências de relações do SnapMirror e do SnapVault. Você pode criar um novo agendamento para aumentar a frequência das transferências de dados devido a atualizações frequentes dos dados, ou pode criar um agendamento menos frequente quando os dados mudam com pouca frequência.

Não é possível configurar agendamentos para relacionamentos síncronos do SnapMirror.

- **Cluster de destino**

  O nome do cluster que você selecionou na guia SnapVault ou na guia SnapMirror da caixa de diálogo Configure Protection.

- **Nome do agendamento**

  O nome que você fornece para o agendamento. Os nomes de agendamento 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 de agendamento não podem incluir os seguintes caracteres: < >.

- **Básico ou Avançado**

  O modo de agendamento que você deseja usar.

  O modo básico inclui os seguintes elementos:

  - Repetir

Com que frequência ocorre uma transferência programada. As opções incluem a cada hora, diariamente e semanalmente.

◦ Dia

Quando a repetição semanal é selecionada, o dia da semana em que a transferência ocorre.

◦ Tempo

Ao selecionar Diário ou Semanal, a hora do dia em que ocorre uma transferência.

O modo avançado inclui os seguintes elementos:

◦ Meses

Uma lista numérica separada por vírgulas que representa os meses do ano. Os valores válidos são de 0 a 11, com zero representando janeiro, e assim por diante. Este elemento é opcional. Deixar o campo em branco implica que as transferências ocorrem todos os meses.

◦ Dias

Uma lista numérica separada por vírgulas 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 úteis

Uma lista numérica separada por vírgulas que representa os dias da semana. Os valores válidos vão 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 ocorra todos os dias da semana. Se um dia da semana for especificado, mas um dia do mês não for especificado, uma transferência ocorrerá apenas no dia da semana especificado, 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 a 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.

Use a caixa de diálogo Criar SnapMirror Policy no Active IQ Unified Manager

A caixa de diálogo Criar política do SnapMirror permite criar uma política para definir a prioridade das transferências do SnapMirror. Você usa políticas para maximizar a eficiência das transferências da origem para o destino.

- **Cluster de destino**

  O nome do cluster que você selecionou na guia SnapMirror da caixa de diálogo Configure Protection.

- **SVM de destino**

O nome da SVM que você selecionou na guia SnapMirror da caixa de diálogo Configure Protection.

- **Nome da política**

  O nome que você fornecer para a nova política. Os nomes de políticas podem conter os caracteres de A a Z, de a a z, de 0 a 9, ponto (.), hífen (-) e sublinhado (_).

- **Prioridade de Transferência**

  A prioridade com que uma transferência é executada para operações assíncronas. Você pode selecionar Normal ou Low. Os relacionamentos de transferência com políticas que especificam uma prioridade de transferência normal são executados antes daqueles com políticas que especificam uma prioridade de transferência low.

- **Comentário**

  Um campo opcional no qual você pode adicionar comentários sobre a política.

- **Reiniciar transferência**

  Indica qual ação de reinicialização executar quando uma transferência é interrompida por uma operação de cancelamento ou qualquer tipo de falha, como uma interrupção de rede. Você pode selecionar uma das seguintes opções:

  - Sempre

    Especifica que uma nova cópia Snapshot seja criada antes de reiniciar uma transferência e, se já existir uma, a transferência seja reiniciada a partir de um ponto de verificação, seguida por uma transferência incremental a partir da cópia Snapshot recém-criada.

  - Nunca

    Especifica que as 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 Configure Protection.

- **Aplicar**

  Aplica suas seleções e inicia o processo de proteção.

Use a caixa de diálogo Criar SnapVault Policy no Active IQ Unified Manager

A caixa de diálogo Create SnapVault Policy permite criar uma política para definir a prioridade das transferências do SnapVault. Você usa políticas para maximizar a eficiência das transferências do volume primário para o volume secundário.

- **Cluster de destino**

  O nome do cluster que você selecionou na aba SnapVault da caixa de diálogo Configure Protection.

- **SVM de destino**

  O nome da SVM que você selecionou na guia SnapVault da caixa de diálogo Configure Protection.

- **Nome da política**

  O nome que você fornecer para a nova política. Os nomes de políticas podem conter os 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 Baixa. Os 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**

  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 Snapshot selecionadas pelo ONTAP que possuem 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 Snapshot e defina uma contagem de retenção.

    - Editar contagem de retenção

      Permite que você altere a contagem de retenção de um rótulo de cópia Snapshot existente. A contagem de retenção deve ser um número entre 1 e 251. A soma de todas as contagens de retenção de todas as regras não pode exceder 251.

    - Excluir

      Permite excluir um rótulo de cópia Snapshot existente.

  - Rótulo da cópia Snapshot

    Exibe o rótulo da cópia Snapshot. Se você selecionar um ou mais volumes com a mesma política local de cópia Snapshot, será exibida uma entrada para cada rótulo na política. Se você selecionar vários volumes que tenham duas ou mais políticas locais de cópia Snapshot, a tabela exibirá todos os rótulos de todas as políticas

◦ Cronograma

Exibe a programação associada a cada rótulo de cópia Snapshot. Se um rótulo tiver mais de uma programação associada a ele, as programações desse rótulo serão exibidas em uma lista separada por vírgulas. Se você selecionar vários volumes com o mesmo rótulo, mas com programações diferentes, a programação exibirá “Várias” para indicar que mais de uma programação está associada aos volumes selecionados.

◦ Contagem de retenção de destino

Exibe o número de cópias Snapshot com o rótulo especificado que são retidas no secundário do SnapVault. 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 locais de cópia Snapshot, a contagem de retenção ficará vazia.

Editar uma relação de proteção no Active IQ Unified Manager

Você pode editar uma relação de proteção existente para alterar a taxa máxima de transferência, a política de proteção ou o cronograma de proteção.

Informações sobre o destino

- **Cluster de destino**

  O nome do cluster de destino selecionado.

- **SVM de destino**

  O nome da SVM selecionada

- **Configurações de relacionamento**

  Permite especificar a taxa de transferência máxima, a política do SnapMirror e o cronograma que a relação de proteção utiliza:

  ◦ Taxa máxima de transferência

  Especifica a taxa máxima de transferência dos dados da transferência completa entre clusters pela rede. Quando selecionado, a largura de banda da rede é limitada ao valor que você especificar. 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 que você especificar deve ser maior que 1 KBps e menor que 4 TBps. Se você optar por não usar uma taxa máxima de transferência, a transferência completa entre relacionamentos será ilimitada. Se o cluster primário e o cluster secundário forem o mesmo, essa configuração fica desativada.

  ◦ Política do SnapMirror

  Especifica a política do SnapMirror do ONTAP para a relação. O padrão é DPDefault.

  ◦ Criar política

  Abre a caixa de diálogo Criar política do SnapMirror, que permite criar e usar uma nova política do SnapMirror.

◦ SnapMirror Agendamento

Especifica a política do ONTAP SnapMirror para a relação. Os agendamentos disponíveis incluem None, 5min, 8hour, daily, hourly e weekly. O padrão é None, indicando que nenhum agendamento está associado à relação. Relações sem agendamentos não têm valores de status de atraso, a menos que pertençam a um serviço de armazenamento.

◦ Criar programação

Abre 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 Configure Protection.

- **Enviar**

  Aplica suas seleções e fecha a caixa de diálogo Edit Relationship.

Utilize a caixa de diálogo Inicializar/Atualizar no Active IQ Unified Manager

A caixa de diálogo Inicializar/Atualizar permite que você execute uma transferência completa pela primeira vez em um novo relacionamento de proteção ou atualize um relacionamento se ele já estiver inicializado e você quiser executar uma atualização incremental manual e não agendada.

Guia Opções de transferência

A guia Opções de transferência permite alterar a prioridade de inicialização de uma transferência e a largura de banda usada durante as transferências.

- **Prioridade de Transferência**

  A prioridade com que a transferência é executada. Você pode selecionar Normal ou Baixa. Os relacionamentos com políticas que especificam uma prioridade de transferência Normal são executados antes daqueles que especificam uma prioridade de transferência Baixa. A opção Normal é selecionada 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 máxima de transferência, a transferência completa 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 os valores especificados durante a configuração ou edição do relacionamento individual

  Quando selecionada, as operações de inicialização e atualização utilizam a taxa de transferência máxima especificada no momento da criação ou edição de cada relacionamento. Este campo está disponível apenas quando vários relacionamentos com taxas de transferência diferentes estão sendo inicializados ou atualizados.

◦ Ilimitado

Indica que não há limitação de largura de banda nas transferências entre relacionamentos. Este campo está disponível apenas quando vários relacionamentos com taxas de transferência diferentes estão sendo inicializados ou atualizados.

◦ Limitar largura de banda para

Quando selecionado, a largura de banda é limitada ao valor que você especificar. Você pode inserir um valor numérico e selecionar kilobytes por segundo (KBps), megabytes por segundo (MBps), gigabytes por segundo (GBps) ou terabytes por segundo (TBps). A taxa de transferência máxima que você especificar deve ser superior a 1 KBps e inferior a 4 TBps.

Guia Cópias Snapshot de origem

A guia Cópias Snapshot de origem exibe as seguintes informações sobre a cópia Snapshot de origem usada para a transferência completa:

- **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 Snapshot**

  Exibe a cópia Snapshot usada para a transferência de dados. Clicar no valor da cópia Snapshot exibe a caixa de diálogo "Select Source Snapshot Copy", na qual você pode selecionar uma cópia Snapshot específica para sua transferência, dependendo do tipo de relação de proteção que você tem e da operação que está executando. A opção de especificar uma cópia Snapshot diferente não está disponível para origens do 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 Initialize/Update.

- **Enviar**

  Salva suas seleções e inicia a tarefa de inicialização ou atualização.

Utilize a caixa de diálogo de ressincronização no Active IQ Unified Manager

A caixa de diálogo Ressincronizar permite que você ressincronize dados em uma relação do SnapMirror ou do SnapVault que foi interrompida anteriormente e, em seguida, o destino foi transformado em um volume de leitura/gravação. Você também pode

ressincronizar quando uma cópia Snapshot comum necessária no volume de origem é excluída, fazendo com que as atualizações do SnapMirror ou do SnapVault falhem.

Aba de opções de ressincronização

A aba Opções de Ressincronização permite definir a prioridade de transferência e a taxa máxima de transferência para o relacionamento de proteção que você está ressincronizando.

- **Prioridade de Transferência**

  A prioridade em que a transferência é executada. Você pode selecionar Normal ou Low. Os 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 que você especificar. 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 máxima de transferência, a transferência completa entre relacionamentos será ilimitada.

Guia Cópias Snapshot de origem

A guia Cópias Snapshot de origem exibe as seguintes informações sobre a cópia Snapshot de origem usada para a transferência completa:

- **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 Snapshot**

  Exibe a cópia Snapshot usada para a transferência de dados. Clicar no valor da cópia Snapshot exibe a caixa de diálogo "Select Source Snapshot Copy", na qual você pode selecionar uma cópia Snapshot específica para a sua transferência, dependendo do tipo de relação 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 Resynchronize.

- **Cancelar**

  Cancela suas seleções e fecha a caixa de diálogo Ressincronizar.

Use a caixa de diálogo Selecionar Cópia de Snapshot da Origem no Active IQ Unified Manager

Você usa a caixa de diálogo Select Source Snapshot Copy para selecionar uma cópia Snapshot específica para transferir dados entre relacionamentos de proteção, ou seleciona o comportamento padrão, que varia dependendo de você estar inicializando, atualizando ou ressincronizando um relacionamento e de o relacionamento ser SnapMirror ou SnapVault.

Padrão

Permite selecionar o comportamento padrão para determinar qual cópia Snapshot será usada para inicializar, atualizar e ressincronizar transferências para relacionamentos do SnapVault e do SnapMirror.

Se você estiver realizando uma transferência do SnapVault, o comportamento padrão de cada operação será o seguinte:

Operação	Comportamento padrão do SnapVault quando a origem é leitura/gravação	Comportamento padrão do SnapVault quando a origem é Proteção de Dados (DP)
Inicializar	Cria uma nova cópia Snapshot e a transfere.	Transfere a última cópia Snapshot exportada.
Atualizar	Transfere apenas cópias Snapshot rotuladas, conforme especificado na política.	Transfere a última cópia Snapshot exportada.
Ressincronizar	Transfere todas as cópias Snapshot rotuladas criadas após a cópia Snapshot comum mais recente.	Transfere a cópia Snapshot rotulada mais recente.

Se você estiver realizando uma transferência do SnapMirror, o comportamento padrão para cada operação é o seguinte:

Operação	Comportamento padrão do SnapMirror	Comportamento padrão do SnapMirror quando o relacionamento é o segundo salto em uma cascata do SnapMirror para o SnapMirror
Inicializar	Cria uma nova cópia Snapshot e a transfere, juntamente com todas as cópias Snapshot criadas antes da nova cópia Snapshot.	Transfere todas as cópias Snapshot da origem.
Atualizar	Cria uma nova cópia Snapshot e a transfere, juntamente com todas as cópias Snapshot criadas antes da nova cópia Snapshot.	Transfere todas as cópias Snapshot.

Operação	Comportamento padrão do SnapMirror	Comportamento padrão do SnapMirror quando o relacionamento é o segundo salto em uma cascata do SnapMirror para o SnapMirror
Ressincronizar	Cria uma nova cópia Snapshot e, em seguida, transfere todas as cópias Snapshot da origem.	Transfere todas as cópias Snapshot do volume secundário para o volume terciário e exclui quaisquer dados adicionados após a criação da cópia Snapshot comum mais recente.

Cópia Snapshot existente

Permite selecionar uma cópia Snapshot existente na lista, caso a seleção de cópia Snapshot seja permitida para essa operação.

- **cópia Snapshot**

  Exibe as cópias Snapshot existentes das quais você pode selecionar uma para transferência.

- **Data de Criação**

  Exibe a data e a hora em que a cópia Snapshot foi criada. As cópias Snapshot são listadas da mais recente para a mais antiga, com a mais recente no topo da lista.

Se você estiver realizando uma transferência do SnapVault e quiser selecionar uma cópia Snapshot existente para transferir de uma origem para um destino, o comportamento de cada operação será o seguinte:

Operação	SnapVault comportamento ao especificar uma cópia Snapshot	Comportamento do SnapVault ao especificar uma cópia Snapshot em uma cascata
Inicializar	Transfere a cópia Snapshot especificada.	A seleção da cópia Snapshot de origem não é compatível com volumes de proteção de dados.
Atualizar	Transfere a cópia Snapshot especificada.	A seleção da cópia Snapshot de origem não é compatível com volumes de proteção de dados.
Ressincronizar	Transfere a cópia Snapshot selecionada.	A seleção da cópia Snapshot de origem não é compatível com volumes de proteção de dados.

Se você estiver realizando uma transferência do SnapMirror e quiser selecionar uma cópia 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 Snapshot	Comportamento do SnapMirror ao especificar uma cópia Snapshot em cascata
Inicializar	Transfere todas as cópias Snapshot na origem, até a cópia Snapshot especificada.	A seleção da cópia Snapshot de origem não é compatível com volumes de proteção de dados.

Operação	Comportamento do SnapMirror ao especificar uma cópia Snapshot	Comportamento do SnapMirror ao especificar uma cópia Snapshot em cascata
Atualizar	Transfere todas as cópias Snapshot na origem, até a cópia Snapshot especificada.	A seleção da cópia Snapshot de origem não é compatível com volumes de proteção de dados.
Ressincronizar	Transfere todas as cópias Snapshot da origem, até a cópia Snapshot selecionada, e depois exclui todos os dados adicionados após a criação da cópia Snapshot comum mais recente.	A seleção da cópia Snapshot de origem não é compatível com volumes de proteção de dados.

Botões de comando

Os botões de comando permitem que você execute as seguintes tarefas:

- **Enviar**

  Confirma suas seleções e fecha a caixa de diálogo Selecionar cópia Snapshot de origem.

- **Cancelar**

  Descarta suas seleções e fecha a caixa de diálogo Selecionar cópia Snapshot de origem.

Reversão da resincronização no Active IQ Unified Manager

Quando uma relação de proteção é interrompida porque o volume de origem está desativado e o destino se torna um volume de leitura/gravação, a ressincronização reversa permite inverter a direção da relação, de modo que o destino se torne a nova origem e a origem se torne o novo destino.

Quando um desastre desabilita o volume de origem na sua relação de proteção, você pode usar o volume de destino para fornecer dados, convertendo-o para leitura/gravação, enquanto repara ou substitui a origem, atualiza a origem e restabelece a relação. Ao executar uma operação de ressincronização reversa, os dados na origem que forem mais recentes do que os dados na cópia Snapshot comum serão excluídos.

Antes da resincronização 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 a resincronização 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 de ressincronização reversa sem iniciar uma operação de ressincronização reversa.

Exibir a relação: visualização de todas as relações no Active IQ Unified Manager

A visualização "Relacionamento: todos os relacionamentos" exibe informações sobre os relacionamentos de proteção no sistema de storage.

Por padrão, ao acessar a página Relationships, o relatório exibido inclui as relações de proteção de nível superior para volumes e VMs de storage. 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 ou reordene colunas na página e exporte os dados da página para um arquivo .csv, .pdf ou .xlsx. Depois de personalizar a página, você pode salvar os resultados como uma visualização personalizada e agendar a geração e o envio regular por e-mail de um relatório desses dados. Por padrão, ao selecionar o menu **Relationships**, o relatório exibido inclui relações de proteção para volumes e VMs de storage no seu datacenter. Você pode usar a opção **Filter** para visualizar apenas os sistemas de storage selecionados, como somente volumes ou somente VMs de storage. O mesmo relatório é exibido na página Storage e apenas para a entidade de storage selecionada. Se você quiser visualizar relações de volume ou de VM de storage, poderá acessar a página **Storage** > **Volumes** > **Relationship: All Relationships** ou acessar **Protection** > **Relationships** > **Relationship: All Relationships** e usar a opção **Relationship Object Type** em **Filter** para filtrar apenas dados de volumes ou VMs de storage.

A página "Relacionamentos" que lista todas as relações de proteção tem o link "Visualizar no System Manager" para o cluster de destino que permite a você visualizar os mesmos objetos no ONTAP System Manager.

- **Status**

  Exibe o status atual da relação de proteção.

  O status pode ser Erro (), Aviso () ou OK ().

- **VM de armazenamento de origem**

  Exibe o nome da SVM de origem. Você pode visualizar mais detalhes sobre a SVM de origem clicando no nome da SVM.

Quando uma SVM existe no cluster, mas ainda não foi adicionada ao inventário do Unified Manager, ou quando a SVM foi criada após a última atualização do cluster, este campo estará vazio. Você deve garantir que a SVM exista ou realizar uma redescoberta no cluster para atualizar a lista de recursos.

- **Fonte**

  Exibe o volume de origem ou a máquina virtual de armazenamento de origem que está sendo protegida com base na sua seleção. Você pode visualizar mais detalhes sobre o volume de origem ou a máquina virtual de armazenamento clicando no nome do volume ou da máquina virtual de armazenamento.

  Se a mensagem `Resource-key not discovered` for exibida, 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 realizar uma redescoberta no cluster para atualizar a lista de recursos.

- **VM de armazenamento de destino**

  Exibe o nome da SVM de destino. Você pode visualizar mais detalhes sobre a SVM de destino clicando no nome da SVM.

- **destino**

  Exibe o nome do volume de destino ou da máquina virtual de armazenamento com base na sua seleção. Você pode visualizar mais detalhes sobre o volume de destino ou a máquina virtual de armazenamento clicando no nome do objeto correspondente.

- **Tipo de objeto de relacionamento**

  Exibe o tipo de objeto usado na relação, como VM de storage, volume e grupo de consistência. Para objetos em uma relação de consistência, a origem e os destinos da relação exibem o grupo de consistência e, ao clicar neles, você vai para a página de LUNs para visualizar a relação.

- **Política**

  Exibe o nome da política de proteção da relação do SnapMirror. Você pode clicar no nome da política para ver os detalhes associados a essa política, incluindo as seguintes informações:

  - Prioridade de transferência

    Especifica a prioridade com que uma transferência é executada para operações assíncronas. A prioridade da transferência é Normal ou Baixa. Transferências com prioridade Normal são agendadas antes das transferências com prioridade Baixa. O padrão é Normal.

  - Ignorar tempo de acesso

    Aplica-se somente a relacionamentos do SnapVault. Isso especifica se as transferências incrementais ignoram arquivos cujo tempo de acesso foi alterado apenas. Os valores são True ou False. O padrão é False.

  - Quando um relacionamento está fora de sincronização

    Especifica a ação que o ONTAP executa quando uma relação síncrona não pode ser sincronizada. As relações StrictSync restringem o acesso ao volume primário se houver falha na sincronização com o volume secundário. As relações Sync não restringem o acesso ao volume primário se houver falha na sincronização com o volume secundário.

- Limite de tentativas

  Especifica o número máximo de tentativas para cada transferência manual ou agendada de uma relação do SnapMirror. O padrão é 8.

- Comentários

  Fornece um campo de texto para comentários específicos sobre a política selecionada.

- SnapMirror Rótulo

  Especifica o rótulo do SnapMirror para o primeiro agendamento associado à política de cópia Snapshot. O rótulo do SnapMirror é usado pelo subsistema SnapVault quando você faz backup de cópias Snapshot em um destino do SnapVault.

- Configuração de retenção

  Especifica por quanto tempo os backups são mantidos, com base no tempo ou no número de backups.

- Cópias Snapshot reais

  Especifica o número de cópias Snapshot neste volume que correspondem ao rótulo especificado.

- Preservar cópias Snapshot

  Especifica o número de SnapVault cópias Snapshot que não são excluídas automaticamente, mesmo que o limite máximo da política seja atingido. Os valores são True ou False. O padrão é False.

- Limiar de aviso de retenção

  Especifica o limite de cópias Snapshot a partir do qual um aviso é enviado para indicar que o limite máximo de retenção está quase atingido.

- **Duração do atraso**

  Exibe o tempo de atraso entre os dados no espelho e os dados na origem.

  A duração do atraso deve ser próxima de 0 segundos ou igual a 0 segundos para relacionamentos StrictSync.

- **Status de lag**

  Exibe o status de atraso para relacionamentos gerenciados e para relacionamentos não gerenciados que possuem um agendamento associado 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 se aplica a relacionamentos síncronos porque não é possível configurar um agendamento.

- **Última atualização bem-sucedida**

  Exibe a hora da última operação bem-sucedida do SnapMirror ou SnapVault.

  A última atualização bem-sucedida não se aplica a relacionamentos síncronos.

- **Relações de constituintes**

  Exibe se existem volumes no objeto selecionado.

- **Tipo de relacionamento**

  Exibe o tipo de relacionamento usado para replicar um volume. Os tipos de relacionamento incluem:

  - Espelho Assíncrono
  - Vault assíncrono
  - Assíncrono MirrorVault
  - StrictSync
  - Sincronizar

- **Status da transferência**

  Exibe o status da transferência da relação de proteção. O status da transferência pode ser um dos seguintes:

  - Abortando

    As transferências do SnapMirror estão habilitadas; no entanto, uma operação de cancelamento 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 não há transferência em andamento.

  - Finalizando

    As transferências do SnapMirror estão habilitadas. Atualmente, o volume está na fase pós-transferência para transferências incrementais do SnapVault.

  - Inativo

    As transferências estão ativadas e nenhuma transferência está em andamento.

  - Em sincronia

    Os dados nos dois volumes na relação síncrona estão sincronizados.

  - Fora de sincronia

Os dados no volume de destino não estão sincronizados com o volume de origem.

- Preparando

  As transferências do SnapMirror estão habilitadas. O volume está atualmente na fase de pré-transferência para transferências incrementais do SnapVault.

- Em fila

  As transferências do SnapMirror estão ativadas. Nenhuma transferência está em andamento.

- Em estado inativo

  As transferências do SnapMirror estão desativadas. Nenhuma transferência está em andamento.

- Colocando em quiescência

  Uma transferência do SnapMirror está em andamento. As transferências adicionais estão desativadas.

- Transferindo

  As transferências do SnapMirror estão ativadas e uma transferência está em andamento.

- Em transição

  A transferência assíncrona de dados da 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 colocadas na fila.

- **Duração da última transferência**

  Exibe o tempo necessário para concluir a última transferência de dados.

  A duração da transferência não se aplica a relacionamentos StrictSync, pois a transferência deve ser simultânea.

- **Último tamanho de transferência**

  Exibe o tamanho, em bytes, da última transferência de dados.

  O tamanho da transferência não se aplica a relacionamentos StrictSync.

- **Mediadores**

  Exibe o status do mediador.

  - Não aplicável

    Se o cluster não oferecer suporte à 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 Mediator

  Se estiver configurado, e se os clusters de origem e de destino forem adicionados no Unified Manager.

- **Estado**

  Exibe o estado da relação do SnapMirror ou do SnapVault. O estado pode ser Não inicializado, SnapMirrored ou Desconectado. Se um volume de origem for selecionado, o estado da relação não se aplica e não é exibido.

- **Integridade da relação**

  Exibe a integridade da relação do cluster.

- **Motivo não íntegro**

  O motivo pelo qual a relação está em um estado não íntegro.

- **Prioridade de Transferência**

  Exibe a prioridade na qual uma transferência é executada. A prioridade da transferência é Normal ou Baixa. As transferências com prioridade Normal são agendadas antes das transferências com prioridade Baixa.

  A prioridade de transferência não se aplica a relacionamentos síncronos, pois todas as transferências são tratadas com a mesma prioridade.

- **Programação**

  Exibe o nome da agenda de proteção atribuída à relação.

  O agendamento não se aplica a relacionamentos síncronos.

- **Versão de replicação flexível**

  Exibe "Sim", "Sim com opção de backup" ou "Nenhum".

- **Cluster de origem**

  Exibe o FQDN, o nome abreviado ou o endereço IP do cluster de origem para a relação do SnapMirror.

- **FQDN do cluster de origem**

  Exibe o nome do cluster de origem para a relação do SnapMirror.

- **Nó de origem**

  Exibe o link do nome do nó de origem para a relação do SnapMirror de um volume e exibe o link da contagem de nós da relação do SnapMirror quando o objeto é uma máquina virtual de armazenamento ou um grupo de consistência.

Na visualização personalizada, ao clicar no link do nome do nó, você pode visualizar e estender a proteção de objetos de armazenamento aos quais os volumes desses grupos de consistência pertencem em uma relação

de sincronização ativa do SnapMirror.

Ao clicar no link de contagem de nós, você vai para a página de nós com os respectivos nós associados a essa relação. Quando a contagem de nós for 0, nenhum valor será exibido, pois não há nós associados à relação.

- **Nó de destino**

  Exibe o link do nome do nó de destino para a relação do SnapMirror de um volume e exibe o link da contagem de nós da relação do SnapMirror quando o objeto é uma máquina virtual de armazenamento ou um grupo de consistência.

  Ao clicar no link de contagem de nós, você vai para a página de nós com os respectivos nós associados a essa relação. Quando a contagem de nós for 0, nenhum valor será exibido, pois não há nós associados à relação.

- **Cluster de destino**

  Exibe o nome do cluster de destino para a relação do SnapMirror.

- **FQDN do cluster de destino**

  Exibe o FQDN, o nome abreviado ou o endereço IP do cluster de destino para a relação do SnapMirror.

- **Protegido por**

  Exibe os diferentes relacionamentos. Nesta coluna, você pode visualizar os relacionamentos de volume e de grupo de consistência para clusters e a ordem das máquinas virtuais de armazenamento, incluindo:

  - SnapMirror
  - DR de VM de armazenamento
  - SnapMirror, DR de VM de armazenamento
  - Grupo de consistência
  - SnapMirror, grupo de consistência.

Informações relacionadas

- Para obter informações sobre a visualização **Relacionamento: MetroCluster**, consulte "Monitoramento de 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 "Relação: visualização da taxa de transferência do último mês".

Exibir a visualização do status de transferência do último mês no Active IQ Unified Manager

A visualização "Relacionamento: status de transferência do último mês" permite analisar as tendências de transferência ao longo do tempo para volumes e VMs de armazenamento em relacionamentos assíncronos. Esta página também exibe se a transferência foi bem-sucedida ou falhou.

Os controles na parte superior da página permitem que você realize buscas para localizar objetos específicos,

crie e aplique filtros para restringir a lista de dados exibidos, adicione, remova ou reordene colunas na página e exporte os dados da página para um arquivo `.csv`, `.pdf` ou `.xlsx`. Depois de personalizar a página, você pode salvar os resultados como uma visualização personalizada e agendar a geração e o envio por e-mail de um relatório desses dados regularmente. Você pode usar a opção **Filter** para visualizar apenas sistemas de armazenamento selecionados, como apenas volumes ou apenas Storage VMs. O mesmo relatório é exibido na página Storage e apenas para a entidade de armazenamento selecionada. Por exemplo, se você quiser visualizar relações de volume, poderá acessar o relatório Relationship: Last 1 Month Transfer Status para as Storage VMs no menu **Storage** > **Storage VMs** > **Relationship: Last 1 Month Transfer Status** ou no menu **Protection** > **Relationships** > **Relationship: Last 1 Month Transfer Status** e usar o **Filter** para visualizar apenas dados de 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.

- **Horário de início da transferência**

  Exibe a hora de início da transferência de volume.

- **Horário de término da transferência**

  Exibe a hora de término da transferência de volume.

- **Duração da transferência**

  Exibe o tempo necessário (em horas) para concluir a transferência do volume.

- **Tamanho da transferência**

  Exibe o tamanho (em MB) do volume transferido.

- **SVM de origem**

  Exibe o nome da máquina virtual de armazenamento (SVM).

- **Cluster de origem**

  Exibe o nome do cluster de origem.

- **SVM de destino**

  Exibe o nome da SVM de destino.

- **Cluster de destino**

Exibe o nome do cluster de destino.

Informações relacionadas

- Para obter informações sobre a visualização **Relacionamento: todos os relacionamentos**, consulte "Relacionamento: visualizar todos os relacionamentos".
- Para obter informações sobre a visualização **Relacionamento:MetroCluster**, consulte "Monitoramento de configurações do MetroCluster".
- Para obter informações sobre a visualização **Relacionamento: todos os relacionamentos**, consulte "Relação: visualização da taxa de transferência do último mês".

Exibir a relação: visualização da taxa de transferência do último mês no Active IQ Unified Manager

A visualização "Taxa de transferência do último mês da relação" permite que você analise a quantidade de dados do volume transferida diariamente para volumes em relações assíncronas. Esta página também fornece detalhes sobre as transferências diárias e o tempo necessário para concluir a operação de transferência para volumes e Storage VMs.

Os controles na parte superior da página permitem que você realize buscas para localizar objetos específicos, crie e aplique filtros para refinar a lista de dados exibidos, adicione, remova ou reordene colunas na página e exporte os dados da página para um arquivo .csv, .pdf ou .xlsx. Após personalizar a página, você pode salvar os resultados como uma visualização personalizada e agendar a geração e o envio regular por e-mail de um relatório desses dados. Por exemplo, se você quiser visualizar os relacionamentos de volume, pode acessar o menu **Armazenamento** > **Volumes** > **Relacionamento: taxa de transferência do último mês** ou o menu **Proteção** > **Relacionamentos** > **Relacionamentos:taxa de transferência do último mês** e usar o **Filtro** para visualizar apenas os dados dos 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.

- **Hora de término**

  Exibe a hora e a data de término da transferência de volume.

Informações relacionadas

- Para obter informações sobre a visualização **Relacionamento:MetroCluster**, consulte "Monitoramento de 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 "Relação: visualização da taxa de transferência do último mês"

Gere relatórios personalizados

Relatórios do Unified Manager

Saiba mais sobre os relatórios do Active IQ Unified Manager

O Active IQ Unified Manager (formerly OnCommand Unified Manager) permite visualizar, personalizar, baixar e agendar relatórios para seus sistemas de storage ONTAP. Os relatórios podem fornecer detalhes sobre a capacidade, a integridade, o desempenho, a segurança e os relacionamentos de proteção do sistema de storage.

A nova funcionalidade de relatórios e agendamento do Unified Manager, introduzida no Active IQ Unified Manager 9.6, substitui o mecanismo de relatórios anterior, descontinuado na versão 9.5 do Unified Manager.

Os relatórios fornecem diferentes visões da sua rede, oferecendo informações práticas sobre capacidade, integridade, desempenho, segurança e dados de proteção. Você pode personalizar suas visualizações mostrando, ocultando e reorganizando colunas, filtrando e classificando dados e pesquisando os resultados. Você pode salvar visualizações personalizadas para reutilização, baixá-las como relatórios e agendá-las como relatórios recorrentes para distribuí-los 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 fazer upload do arquivo do Excel para usá-lo sempre que o relatório for agendado e compartilhado.

Além de gerar relatórios a partir da interface de usuário, você pode extrair dados de integridade, segurança e desempenho do Unified Manager usando estes métodos adicionais:

- Utilizando a Conectividade Aberta de Banco de Dados (ODBC) e ferramentas ODBC para acessar diretamente o banco de dados e obter informações do cluster
- Executando as APIs REST do Unified Manager para retornar as informações que você deseja revisar

A partir desta versão do Active IQ Unified manager, as seguintes melhorias foram implementadas nos relatórios:

- Um e-mail com o relatório é enviado conforme a programação configurada. Mesmo ao gerar um relatório sob demanda, você receberá um e-mail.
- O nome do arquivo do relatório e os metadados do relatório incluem o nome do host de onde o relatório foi gerado. Mesmo que alguém altere o nome do arquivo, ainda é possível identificar o nome do host de onde o relatório foi gerado graças a essa melhoria.

Pontos de acesso para geração de relatórios

Descubra três maneiras de acessar os recursos de geração de relatórios no Active IQ Unified Manager

Você pode coletar informações no Unified Manager sobre seus clusters para criar relatórios a partir da interface de usuário, de consultas ao banco de dados MySQL e de APIs REST.

Estas seções descrevem a geração de relatórios e o agendamento no Unified Manager por meio da interface

de usuário.

Existem três maneiras de acessar os recursos de geração de relatórios oferecidos pelo Unified Manager:

- Extração de dados diretamente das páginas de inventário na interface de usuário.
- Usando Open Database Connectivity (ODBC) e ferramentas ODBC para acessar todos os objetos disponíveis.
- Executando as APIs REST do Unified Manager para retornar as informações que você deseja revisar.

Estas seções descrevem a geração de relatórios e o agendamento no Unified Manager por meio da interface de usuário.

Acesse bancos de dados para gerar relatórios personalizados no Active IQ Unified Manager

O Unified Manager utiliza um banco de dados MySQL para armazenar dados dos clusters que ele está monitorando. Os dados são persistidos em diversos esquemas no banco de dados MySQL.

Todos os dados tabulares dos seguintes bancos de dados estão disponíveis:

Banco de dados	Descrição
netapp_model	Dados sobre os objetos nos controladores ONTAP.
netapp_model_view	Dados sobre os objetos nos controladores ONTAP, adequados para uso em ferramentas de geração de relatórios.
netapp_performance	Contadores de desempenho específicos do cluster.
ocum	Dados e informações do aplicativo Unified Manager para dar suporte à filtragem da interface de usuário, à classificação e ao cálculo de alguns campos derivados.
ocum_report	Dados para configuração do inventário e informações relacionadas à capacidade.
ocum_report_birt	Visualizações de dados relacionados à configuração de inventário e à capacidade, adequadas para uso em ferramentas de relatório.
opm	Configurações de desempenho e informações sobre limites.
scalemonitor	Dados sobre a integridade do aplicativo Unified Manager e os problemas de desempenho.
vmware_model	Dados de objetos do VMware para datastores hospedados no storage da NetApp.
vmware_model_view	Visualizações de dados de objetos VMware para datastores hospedados no storage da NetApp, adequadas para uso em ferramentas de relatório.
vmware_performance	Dados do contador de desempenho do VMware para datastores hospedados no storage da NetApp.

Um usuário de relatórios, um usuário do banco de dados com a função Report Schema, pode acessar os dados nessas tabelas. Esse usuário tem acesso somente leitura a relatórios e outras visualizações do banco de dados diretamente do banco de dados do Unified Manager. Observe que esse usuário não tem permissão para acessar nenhuma tabela que contenha dados de usuário ou informações de credenciais do cluster.

Use as APIs REST do Active IQ Unified Manager para geração de relatórios

Você pode usar APIs REST para ajudar a gerenciar seus clusters, visualizando as informações de integridade, capacidade, desempenho e segurança coletadas pelo Unified Manager.

As APIs REST são expostas por meio da página web do Swagger. Você pode acessar a página web do Swagger para exibir a documentação da API REST do Unified Manager, bem como para emitir manualmente uma chamada de API. Na interface web do Unified Manager, na barra de menus, clique no botão **Ajuda** e selecione **Documentação da API**. Para obter informações sobre as APIs REST do Unified Manager, consulte "Primeiros passos com as APIs REST do Active IQ Unified Manager".

Você precisa ter a função de Operador, Administrador de storage ou Administrador de aplicativos para acessar as APIs REST.

Compreenda os relatórios no Active IQ Unified Manager

Os relatórios exibem informações detalhadas sobre armazenamento, rede, qualidade do serviço e relacionamentos de proteção, ajudando você a identificar e resolver problemas potenciais 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 visualização no Excel para personalizá-la usando recursos avançados do Excel e, em seguida, carregar esse arquivo de volta para o Unified Manager. Se você agendar um relatório usando essa visualização, ele usará o arquivo do Excel que você carregou para criar relatórios robustos que você poderá compartilhar.

Você pode gerenciar todos os relatórios que foram agendados na página Agendamento de Relatórios.

> Você precisa ter a função de Application Administrator ou Storage Administrator para gerenciar relatórios.

Você pode baixar relatórios como arquivos CSV (valores separados por vírgula), Excel ou PDF.

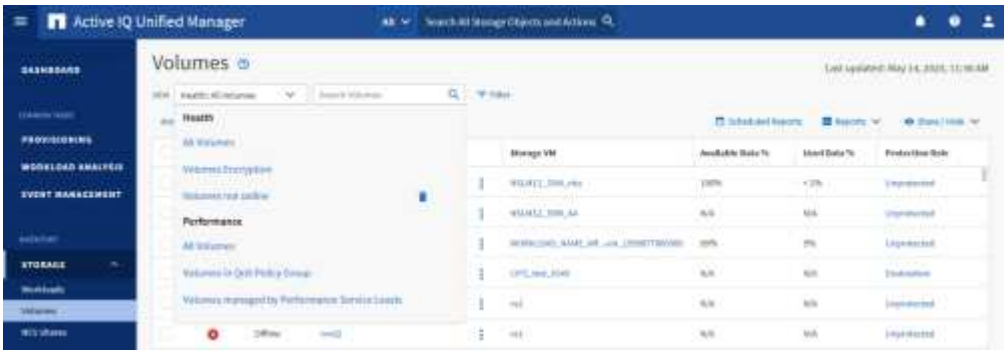
Compreenda a relação entre visualização e relatório no Active IQ Unified Manager

As visualizações e as páginas de inventário se transformam em relatórios quando você as baixa ou agenda.

Você pode personalizar e salvar visualizações e páginas de inventário para reutilização. Quase tudo que você pode visualizar no Unified Manager pode ser salvo, reutilizado, personalizado, agendado e compartilhado como um relatório.

No menu suspenso de visualização, os itens com o ícone de exclusão são visualizações personalizadas existentes que você ou outro usuário criou. Os itens sem ícone são visualizações padrão fornecidas com o Unified Manager. As visualizações padrão não podem ser modificadas nem excluídas.

- Se você excluir uma visualização personalizada da lista, também excluirá todos os arquivos do Excel ou relatórios agendados que usam essa visualização.
- Se você alterar uma visualização personalizada, os relatórios que usam essa visualização refletirão a alteração na próxima vez que o relatório for gerado e enviado por e-mail de acordo com o agendamento de relatórios. Ao alterar visualizações, certifique-se de que suas alterações funcionem com quaisquer personalizações do Excel associadas 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 visualização.



Somente usuários com a função de Application Administrator ou Storage Administrator podem ver o ícone de exclusão, alterar ou excluir uma visualização ou alterar ou excluir um relatório agendado.

Saiba mais sobre os tipos de relatórios no Active IQ Unified Manager

Esta tabela fornece uma lista completa das visualizações e páginas de inventário disponíveis como relatórios que você pode personalizar, baixar e agendar.

Relatórios do Active IQ Unified Manager

Tipo	Objeto de storage ou de rede
Capacidade	Clusters Agregados Volumes Qtrees
Saúde	Clusters Nós Agregados VMs de armazenamento Volumes Compartilhamentos SMB/CIFS Compartilhamentos NFS

Tipo	Objeto de storage ou de rede
Desempenho	Clusters Nós Agregados VMs de armazenamento Volumes LUNs Namespaces NVMe Interfaces de rede (LIFs) Portas
Qualidade do serviço	Grupos de políticas de QoS tradicionais Grupos de políticas de QoS adaptativa Grupos de políticas de nível de serviço de desempenho
Relações de proteção de volume (disponíveis na página Volumes)	Todos os relacionamentos Status da transferência no último mês Taxa de transferência do último 1 mês
Segurança	VMs de armazenamento Clusters

Compreenda as limitações de geração de relatórios no Active IQ Unified Manager

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 cronograma e os destinatários de relatórios existentes que foram criados e importados (como arquivos .rptdesign) no Unified Manager 9.5 e em versões anteriores. Se você personalizou algum dos relatórios padrão fornecidos com Unified Manager 9.5 ou versões anteriores, esses relatórios personalizados não serão importados para a nova ferramenta de relatórios.

Se precisar editar relatórios existentes importados de arquivos .rptdesign, faça um dos seguintes procedimentos e remova o relatório importado:

- criar uma nova visualização e agendar um relatório a partir dessa visualização (preferencial)
- passe o cursor 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.

Relação entre cronograma e relatório

Você pode criar vários agendamentos diferentes com qualquer combinação de destinatários para cada relatório salvo. No entanto, não é possível 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 alterem visualizações ou agendamentos salvos.

Relatórios de eventos

Embora seja possível personalizar a visualização de eventos e baixar o relatório resultante em formato CSV, não é possível agendar a geração e a distribuição de relatórios recorrentes de eventos.

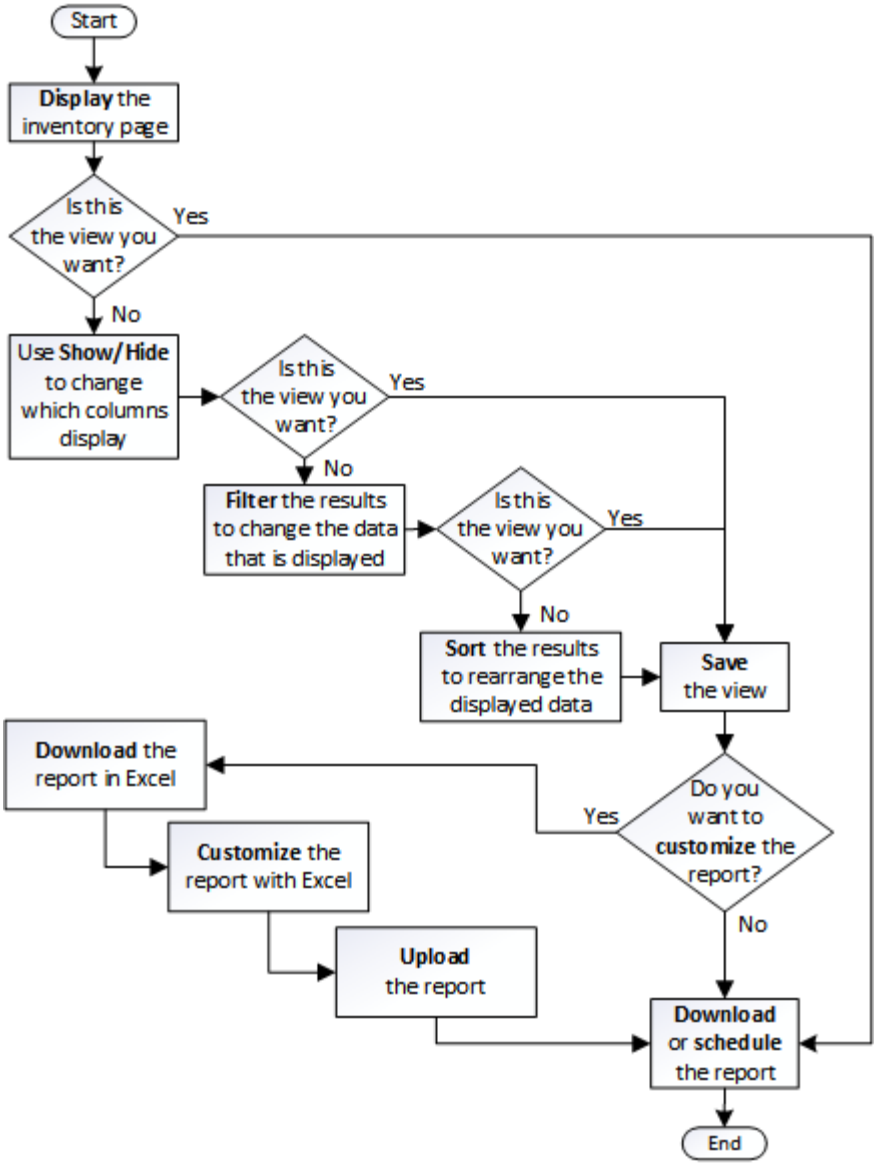
Anexos do relatório

Os relatórios não podem ser enviados no corpo de um e-mail. Em vez disso, são enviados apenas como anexos em PDF, Excel ou CSV.

Trabalhe com relatórios

Compreenda os fluxos de trabalho de relatórios no Active IQ Unified Manager

Árvore de decisão que descreve o fluxo de trabalho do relatório.



Comece a gerar relatórios no Active IQ Unified Manager

Crie um relatório personalizado de exemplo para experimentar a exploração de visualizações e o agendamento de relatórios. Este relatório de início rápido encontra uma lista de volumes que você pode querer mover para a camada da nuvem, pois 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 compartilhá-lo uma vez por semana.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado os agregados do FabricPool e ter volumes nesses agregados.

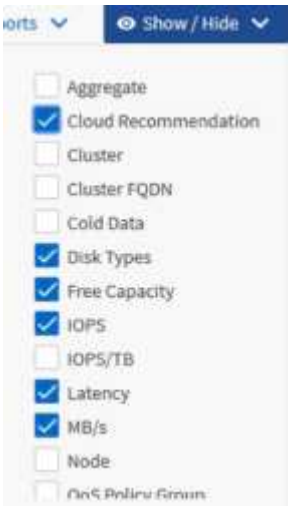
Siga os passos abaixo para:

- Abra a visualização padrão

- Personalize as colunas filtrando e classificando os dados
- Salvar a visualização
- Agende a geração de um relatório para a visualização personalizada

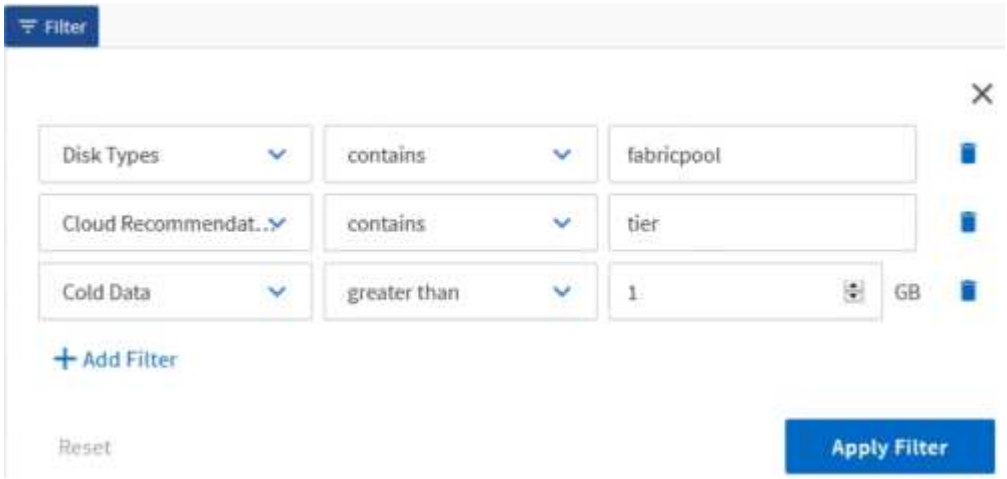
Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Desempenho** > **Todos os volumes**.
3. Clique em **Mostrar/Ocultar** para garantir que a coluna “Disk Types” apareça na visualização.



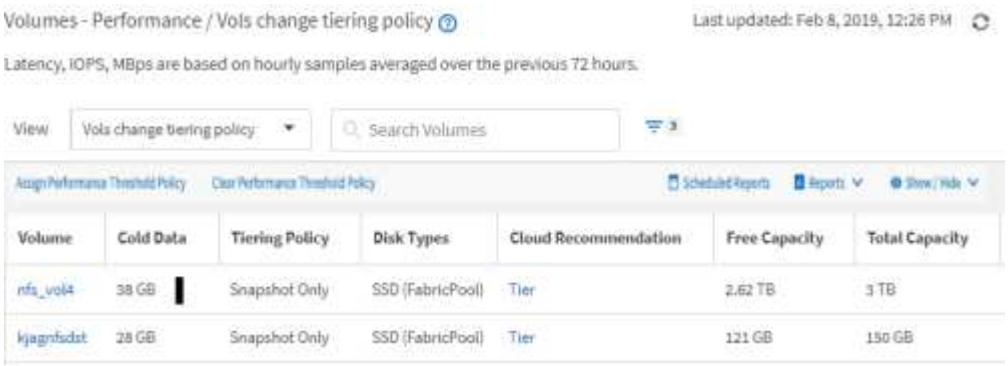
Adicione ou remova outras colunas para criar uma visualização que contenha os campos importantes para o seu relatório.

4. Arraste a coluna “Tipos de disco” para junto da coluna “Recomendação de nuvem”.
5. Clique no ícone de filtro para adicionar os três filtros a seguir e, em seguida, clique em **Apply Filter**:
   - Tipos de disco contém o FabricPool
   - A recomendação de nuvem contém nível
   - Dados frios maiores que 10 GB



Observe que cada filtro é combinado com um operador lógico AND, de forma que todos os volumes retornados devem atender 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 forma que os volumes com mais dados frios apareçam no topo da visualização.
7. Quando a visualização é personalizada, o nome da visualização é "Visualização não salva". Dê à visualização um nome que reflita o que ela está mostrando, por exemplo “Vols change tiering policy”. Quando terminar, clique na marca de seleção ou pressione **Enter** para salvar a visualização com o novo nome.



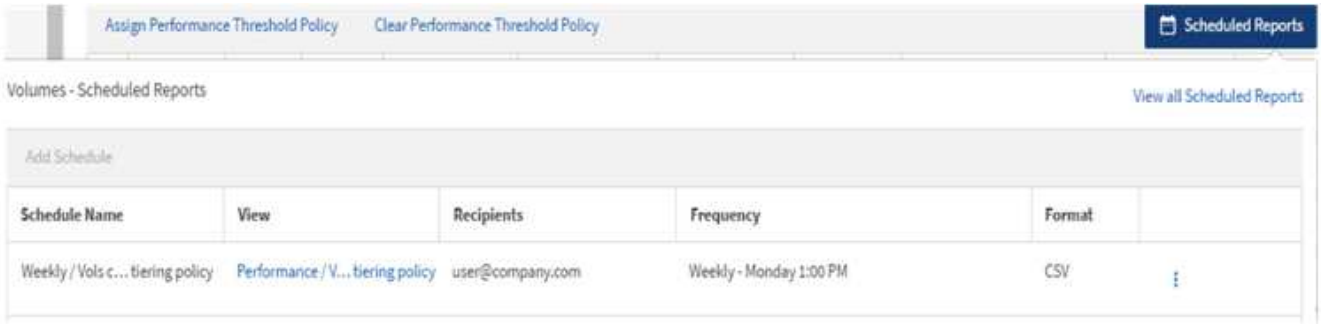
8. Baixe o relatório como um arquivo **CSV**, **Excel** ou **PDF** para visualizar o resultado antes de agendá-lo ou compartilhá-lo.

   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, ordenações, tabelas dinâmicas ou gráficos, baixando a visualização como um arquivo do Excel. Depois de abrir o arquivo no Excel, use os recursos avançados para personalizar seu relatório. Quando estiver satisfeito, faça upload do arquivo do Excel. Esse arquivo, com suas personalizações, é aplicado à visualização quando o relatório é executado.

   Para obter mais informações sobre como personalizar relatórios usando o Excel, consulte *Exemplos de relatórios do Microsoft Excel*.

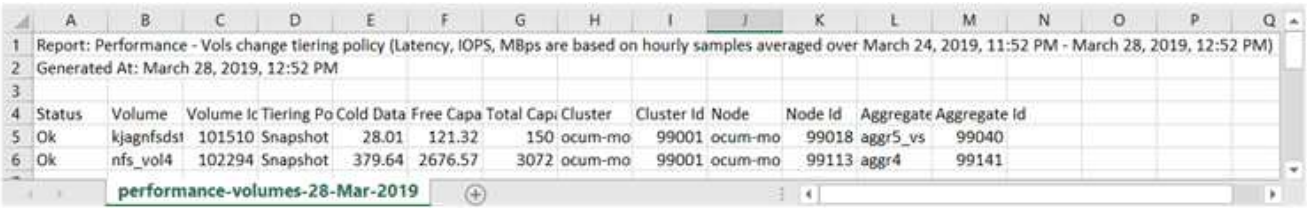
9. Clique no botão **Relatórios Agendados** na página de inventário. Todos os relatórios agendados relacionados ao objeto, neste caso volumes, aparecerão na lista.



10. Clique em **Adicionar agendamento** para adicionar uma nova linha à página Agendamentos de relatório, para que você possa definir as características do agendamento do novo relatório.
11. Insira um nome para o relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

O relatório de exemplo a seguir está em formato CSV:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:52 PM - March 28, 2019, 12:52 PM)																
2	Generated At: March 28, 2019, 12:52 PM																
3																	
4	Status	Volume	Volume Ic	Tiering Po	Cold Data	Free Capa	Total Capa	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id				
5	Ok	kjagnfsdst	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040				
6	Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141				

performance-volumes-28-Mar-2019

O relatório de exemplo a seguir está em formato PDF:



Com base nos resultados apresentados no relatório, você pode usar o ONTAP System Manager ou a ONTAP CLI para alterar a política de armazenamento em camadas para “auto” ou “all” em determinados volumes, a fim de descarregar mais dados inativos para a camada de nuvem.

Pesquise um relatório agendado no Active IQ Unified Manager

Você pode pesquisar relatórios agendados por nome, nome da visualização, 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 por …	Tente …
Nome do agendamento	Digite parte do nome do cronograma do relatório.
Nome da vista	Digite parte do nome da visualização do relatório. As visualizações padrão e as visualizações 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 no cabeçalho de uma coluna para classificar os relatórios em ordem crescente ou decrescente por essa coluna, como nome do agendamento ou formato.

Personalize relatórios

Personalize relatórios no Active IQ Unified Manager

Existem muitas maneiras de personalizar as visualizações para que você possa criar um relatório que contenha todas as informações necessárias para gerenciar seus clusters do 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-os por uma coluna específica em ordem crescente ou decrescente.

A partir do Unified Manager 9.8, você também pode baixar a visualização no Excel para personalizá-la usando recursos avançados. Quando terminar, carregue o arquivo do Excel personalizado. Se você agendar um relatório usando essa visualização, ele usará o arquivo do Excel personalizado para criar relatórios robustos que você poderá compartilhar.

Para obter mais informações sobre como personalizar relatórios usando o Excel, consulte *Exemplos de relatórios do Microsoft Excel*.

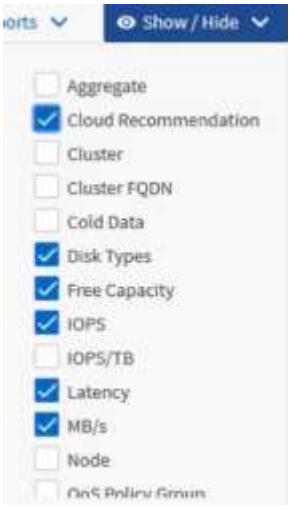
Você precisa ter a função de Application Administrator ou Storage Administrator para gerenciar relatórios.

Personalize as colunas em um relatório no Active IQ Unified Manager

Use **Mostrar/Ocultar** para escolher as colunas que você 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.



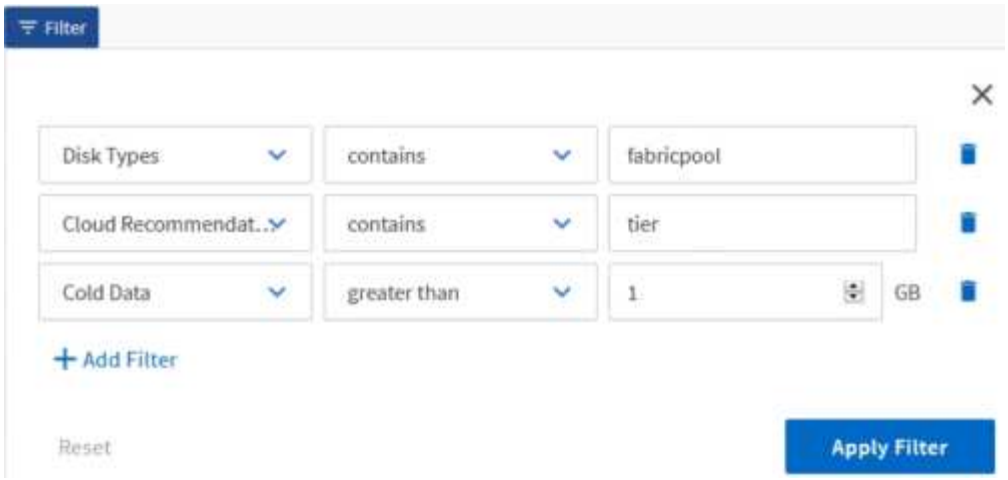
2. Na página de inventário, arraste as colunas para reorganizá-las na ordem desejada em seu relatório.
3. Dê um nome à visualização não salva para salvar suas alterações.

Filtrar dados no Active IQ Unified Manager

Filtre os dados para garantir que os resultados correspondam aos requisitos do seu relatório. A filtragem permite exibir apenas os dados do seu interesse.

Passos

1. Clique no ícone de filtro para adicionar filtros e refinar os resultados que você deseja visualizar e, em seguida, clique em **Aplicar filtro**.



2. Dê um nome à visualização não salva para salvar suas alterações.

Classificar dados no Active IQ Unified Manager

Para classificar os resultados, clique em uma coluna e indique a ordem crescente ou decrescente. A classificação dos dados prioriza as informações necessárias para o relatório.

Passos

1. Clique na parte superior de uma coluna para classificar os resultados, de forma que as informações mais importantes apareçam no topo da visualização.
2. Dê um nome à visualização não salva para salvar suas alterações.

Pesquise para refinar sua visualização no Active IQ Unified Manager

Após obter a visualização desejada, você pode refinar ainda mais os resultados usando o campo Search para se concentrar nos resultados que deseja incluir no relatório.

Passos

1. Abra a visualização personalizada ou padrão que você deseja usar como base para o seu relatório.
2. Digite no campo de pesquisa para refinar os dados listados na visualização. Você pode inserir dados parciais em qualquer uma das colunas exibidas. Por exemplo, se 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. Dê um nome à visualização não salva para salvar suas alterações.

Utilize o Excel para personalizar seu relatório no Active IQ Unified Manager

Após 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.

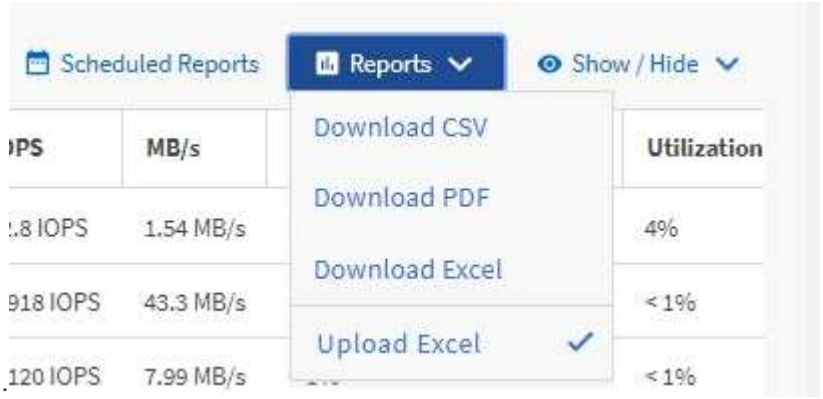
Antes de começar

Você só pode enviar um arquivo de pasta de trabalho do Excel com a extensão .xlsx.

Por exemplo, alguns recursos avançados do Excel que você pode usar no seu relatório incluem:

- Ordenação em várias colunas
- Filtragem complexa
- Tabelas dinâmicas
- Gráficos

- O arquivo Excel baixado usa o nome de arquivo padrão para a visualização, não o nome que você salvou.
  - O formato é `<View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx`.
  - Por exemplo, uma visualização personalizada salva chamada `Volumes-not online` tem o nome de arquivo `health-volumes-05-May-2020-19-18-00.xlsx` se for salva naquele dia e horário.
- Você pode adicionar planilhas ao arquivo do Excel, mas não altere as planilhas existentes.
  - Não altere as planilhas, os dados e as informações existentes. Em vez disso, copie os dados para uma nova página que você criará.
  - Uma exceção à regra acima é que você pode criar fórmulas na página “data”. Use as fórmulas da página `data` para criar gráficos em novas páginas.
  - Não dê a uma nova planilha o nome de data ou info.
- Se existir um arquivo Excel personalizado, haverá uma marca de seleção ao lado do item de menu **Reports** > **Upload Excel**. Ao baixar o arquivo Excel, a versão com as personalizações será usada.



Passos

1. Abra a visualização padrão, personalizada ou salva que você deseja usar como base para o seu relatório.
2. Selecione **Reports** > **Download 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 trabalhar em outro local, salve o arquivo novamente no local original usando o nome original antes de carregá-lo.
5. Personalize o arquivo usando recursos do Excel, como ordenações 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 do arquivo.
7. Envie para você um relatório de teste usando o recurso **Relatórios Agendados**.

Baixe relatórios no Active IQ Unified Manager

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 **Reports** para baixar o relatório em um dos seguintes formatos:

Escolha	Para…
Baixar CSV	Salve o relatório como um arquivo de valores separados por vírgula (CSV).
Baixar PDF	Salve o relatório como um arquivo .pdf.
Baixe o Excel	Salve o relatório como um arquivo do Microsoft Excel (XLSX).

Agendar relatórios

Agende relatórios no Active IQ Unified Manager

Depois de obter uma visualização que deseja reutilizar e compartilhar como um relatório, você pode agendá-la usando o Active IQ Unified Manager. É possível gerenciar relatórios agendados, alterando os destinatários e a frequência de distribuição para cada agendamento de relatório.

É possível agendar a maioria das visualizações ou páginas de inventário no Unified Manager. As exceções são os eventos, que são relatórios que você pode baixar como arquivos CSV, mas não é possível 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 poderá carregar o arquivo do Excel para usá-lo sempre que o relatório for agendado e compartilhado.

Você pode agendar as visualizações incorporadas ou as visualizações que 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 para ver o relatório como seus destinatários o verão.

Agende um relatório

Agende um relatório no Active IQ Unified Manager

Depois de ter uma visualização ou um arquivo do Excel que deseja programar para geração e distribuição regulares, você pode agendar o relatório.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você deve ter configurado as definições do servidor SMTP na página **Geral** > **Notificações** para que o mecanismo de geração 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 juntamente com os e-mails gerados.

Siga as etapas a seguir para testar e agendar a geração de um relatório para uma visualização. 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 visualização de rede padrão que mostra o desempenho da LIF. No painel de navegação esquerdo, clique em **Rede > Interfaces de Rede**.
2. Personalize a visualização conforme necessário usando os recursos incorporados do Unified Manager.
3. Após personalizar a visualização, você pode fornecer um nome exclusivo no campo **View** e clicar na marca de seleção para salvá-la.



4. Você pode usar os recursos avançados do Microsoft® Excel para personalizar seu relatório. Para obter detalhes, consulte "Utilizando o Excel para personalizar seu relatório".
5. Para visualizar o resultado antes de agendá-lo ou compartilhá-lo:

Opção	Descrição
Se você usou o Excel para personalizar o relatório	Visualize o arquivo do Excel já baixado.
Caso não tenha utilizado o Excel para personalizar o relatório	Faça o download do 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).

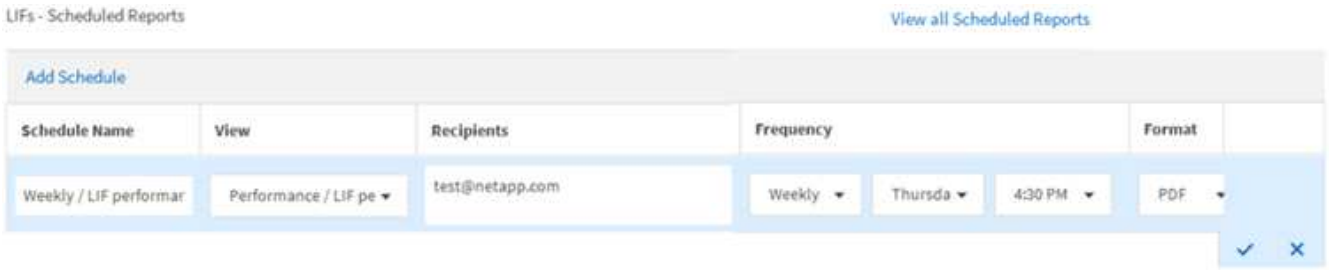
6. Se estiver satisfeito com o relatório, clique em **Scheduled Reports**.
7. Na página Agendamentos de Relatórios, clique em **Adicionar Agendamento**.
8. Aceite o nome padrão, que é uma combinação do nome da visualização e da frequência, ou personalize o **nome da programação**.
9. Para testar o relatório agendado pela primeira vez, adicione apenas você 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

Diariamente, **Semanalmente** ou **Mensalmente**.

11. Selecione o formato, **PDF**, **CSV** ou **XSLX**.

> Para relatórios em que você usou o Excel para personalizar o conteúdo, selecione sempre **XSLX**.

12. Clique na marca de seleção (✓) para salvar o agendamento do relatório.



O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados de acordo com a frequência programada.

Agende relatórios .rptdesign importados no Active IQ Unified Manager

Você pode agendar relatórios existentes que foram criados e importados em uma versão anterior do Unified Manager.

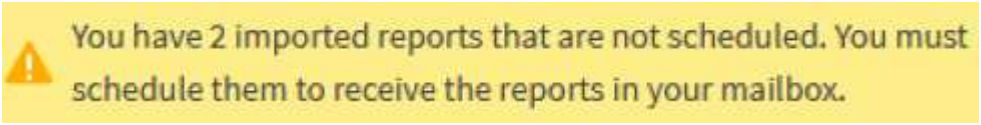
O agendamento de relatórios importados requer o seguinte:

- 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

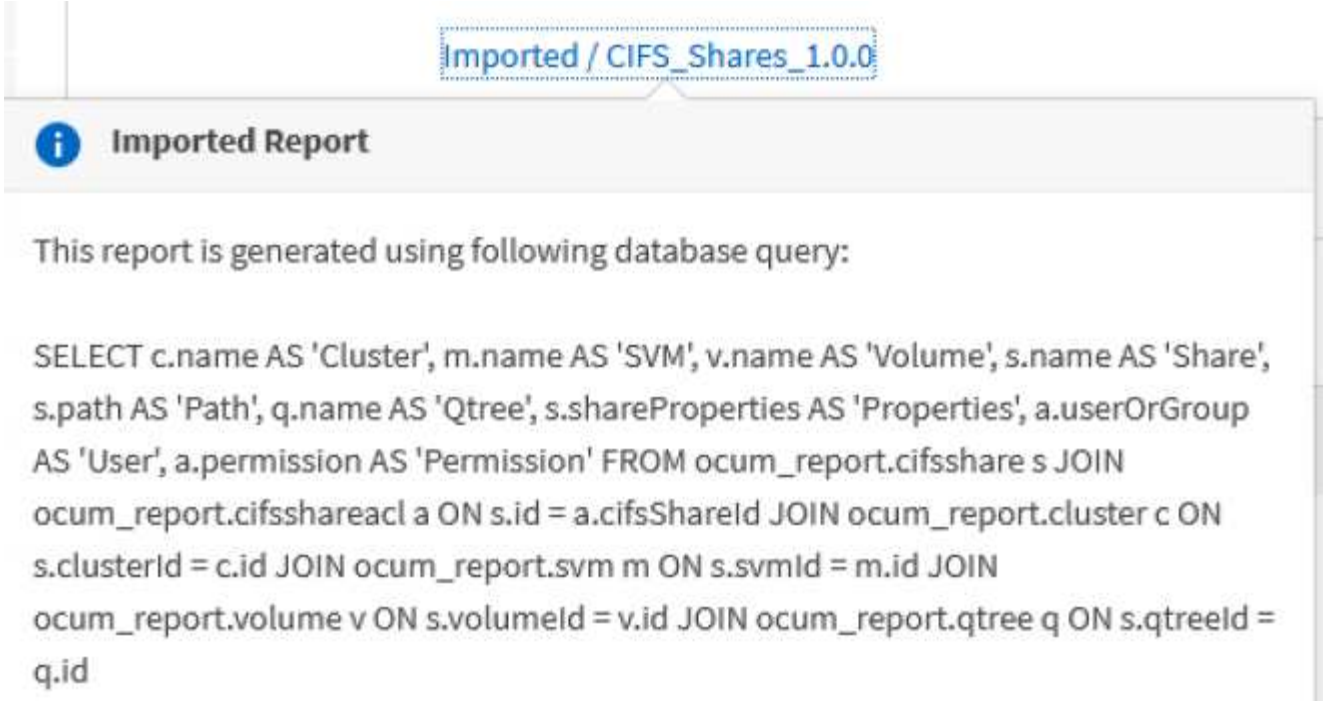
Após a atualização para o Unified Manager 9.6 GA ou posterior, a página "Agendamentos de Relatórios" lista os relatórios importados. Você pode editar o agendamento desses relatórios para especificar os endereços de e-mail dos destinatários, a frequência e o formato (PDF ou CSV). Caso contrário, você não pode editar nem visualizar esses relatórios na UI do Unified Manager.

Passos

1. Abra a página Agendamentos de Relatórios. Se você tiver importado relatórios, uma mensagem aparecerá.



2. Clique no nome **View** para exibir a consulta SQL usada para gerar o relatório.



3. Clique no ícone mais ⋮, clique em **Edit**, defina os detalhes do agendamento do relatório e salve o relatório.

Você também pode excluir quaisquer relatórios indesejados no ícone "Mais" ⋮.

Gerenciar cronogramas de relatórios

Gerencie agendamentos de relatórios no Active IQ Unified Manager

Você pode gerenciar seus agendamentos de relatórios na página Agendamentos de Relatórios. Você pode visualizar, modificar ou excluir agendamentos existentes.

Antes de começar

Não é possível agendar novos relatórios na página "Agendamentos de Relatórios". Você só pode adicionar relatórios agendados nas páginas de inventário de objetos.

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Agendamentos de relatórios**.
2. Na página Programações de relatórios:

Se você quiser…	Então…
Ver um agendamento existente	Navegue pela lista de relatórios existentes usando as barras de rolagem e os controles de página.

Se você quiser…	Então…
Editar um cronograma existente	a. Clique no ícone Mais ⋮ para a programação que você deseja usar. b. Clique em **Editar**. c. Faça as alterações necessárias. d. Clique na marca de seleção para salvar suas alterações.
Excluir um agendamento existente	a. Clique no ícone Mais ⋮ para a programação que você deseja usar. b. Clique em **Delete**. c. Confirme sua decisão.

Edite relatórios agendados no Active IQ Unified Manager

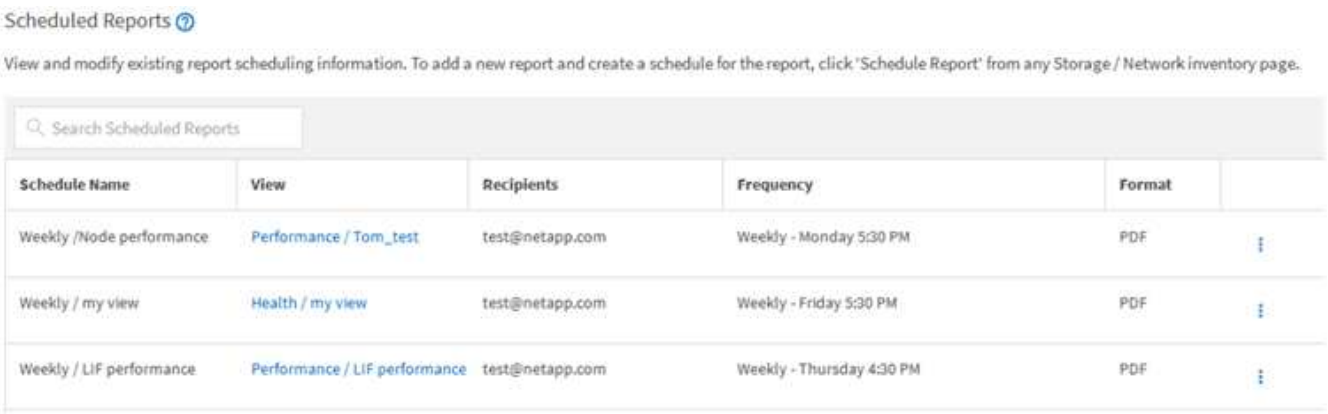
Depois de agendar os relatórios, você poderá editá-los na página de agendamento de relatórios.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Agendamentos de relatórios**.



Se você tiver as permissões adequadas, poderá alterar qualquer relatório e seu agendamento no sistema.

2. Clique no ícone "Mais" ⋮ da programação que você deseja alterar.
3. Clique em **Editar**.
4. Você pode alterar o **Nome da Programação**, a lista de **Destinatários**, a **Frequência** e o **Formato** da programação do relatório.
5. Ao concluir, clique na marca de seleção para salvar suas alterações.

Excluir relatórios agendados no Active IQ Unified Manager

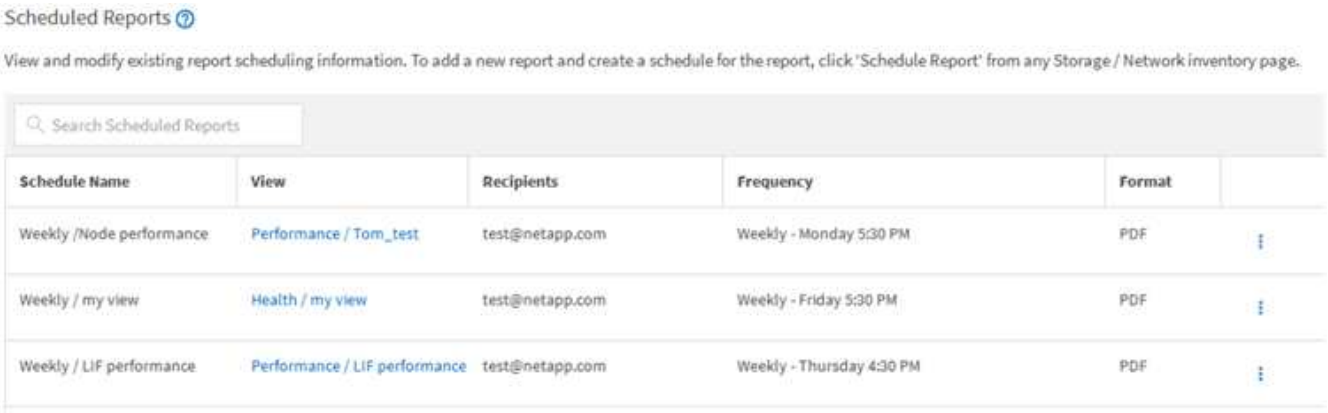
Depois de agendar os relatórios, você pode excluí-los na página de Agendamento de Relatórios.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Agendamentos de relatórios**.



> Se você tiver as permissões adequadas, poderá remover qualquer relatório e seu respectivo agendamento no sistema.

2. Clique no ícone "Mais" ⋮ da programação que você deseja remover.
3. Clique em **Delete**.
4. Confirme sua decisão.

   O relatório agendado é removido da lista e não será mais gerado nem distribuído de acordo com a programação definida.

> Se você excluir uma visualização personalizada da página de inventário, todos os arquivos personalizados do Excel ou relatórios agendados que usam essa visualização também serão excluídos.

Exemplos de relatórios personalizados

Entenda os exemplos de relatórios personalizados no Active IQ Unified Manager

Esses exemplos de relatórios personalizados são comumente usados para ajudar você a identificar possíveis problemas e responder a possíveis questões antes que os problemas ocorram.

A lista de relatórios nesta seção não é exaustiva e será ampliada com o tempo. Você pode sugerir a inclusão de relatórios personalizados nesta seção, enviando seu feedback sobre a documentação.

Você precisa ter a função de Application Administrator ou Storage Administrator para gerenciar relatórios.

Personalize os relatórios de armazenamento do cluster

Crie um relatório para visualizar a capacidade por modelo de cluster no Active IQ Unified Manager

Você pode criar um relatório para analisar a capacidade de storage e a utilização de clusters com base no modelo do sistema de storage.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada que mostre a capacidade por modelo de cluster e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Clusters**.
2. No menu Exibir, selecione **Capacidade** > **Todos os Clusters**.
3. Selecione **Show/Hide** para remover quaisquer colunas, como “Cluster FQDN” e “OS Version”, que você não deseja no relatório.
4. Arraste as colunas “Total Raw Capacity”, “Model/Family” e as três colunas de agregado para perto da coluna “Cluster”.
5. Clique na parte superior da coluna “Model/Family” para classificar os resultados por tipo de cluster.
6. Salve a visualização com um nome específico que reflita o que ela está exibindo, por exemplo, “Capacidade por Modelo de Cluster”.
7. Clique no botão **Relatórios Agendados** na página de inventário.
8. Clique em **Add Schedule** para adicionar uma nova linha à página **Report Schedules**, para que você possa definir as características do agendamento para o novo relatório.
9. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode querer adicionar mais capacidade a determinados clusters ou atualizar modelos de cluster mais antigos.

Identificar clusters com capacidade LUN não alocada no Active IQ Unified Manager

Você pode criar um relatório para encontrar os clusters com a maior capacidade de LUN não alocada, superior a 0,5 TB, para ajudar a identificar onde você pode adicionar cargas de trabalho adicionais.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada que mostre os clusters com a maior

capacidade de LUN não alocada e, em seguida, agende a geração de um relatório para essa visualização.

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 as colunas que você não quer no relatório.
4. Arraste a coluna “Unallocated LUN Capacity” para perto da coluna “HA Pair”.
5. Clique no ícone de filtro, adicione o seguinte filtro e, em seguida, clique em **Apply Filter**:
   - Capacidade de LUN não alocada superior a 0,5 TB
6. Clique na parte superior da coluna “Unallocated LUN Capacity” para classificar os resultados pela maior quantidade de capacidade de LUN não alocada.
7. Salve a visualização com um nome específico que reflita o que ela está mostrando, por exemplo “Maior capacidade de LUN não alocada” e clique na marca de seleção (✓).
8. Clique no botão **Relatórios Agendados** na página de inventário.
9. Clique em **Adicionar Cronograma** para adicionar uma nova linha à página Cronogramas de Relatório, para que você possa definir as características do agendamento do novo relatório.
10. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode optar por usar a capacidade de LUN não alocada do cluster.

Crie um relatório para visualizar os pares de HA com a maior capacidade disponível no Active IQ Unified Manager

Você pode criar um relatório para encontrar os pares de alta disponibilidade (HA) com maior capacidade para provisionar novos volumes e LUNs.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para criar uma visualização personalizada que exiba pares de alta disponibilidade (HA) classificados pela maior capacidade disponível para provisionar novos volumes e LUNs e depois agende a geração de um relatório para essa visualização.

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 as colunas que você não quer no relatório.
4. Arraste a coluna “Aggregate Unused Capacity” para perto da coluna “HA Pair”.
5. Clique no ícone de filtro, adicione o seguinte filtro e, em seguida, clique em **Apply Filter**:
   - Capacidade não utilizada do agregado superior a 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 do agregado menos utilizado”, e clique na marca de seleção (✓).
8. Clique no botão **Relatórios Agendados** na página de inventário.
9. Clique em **Adicionar Cronograma** para adicionar uma nova linha à página Cronogramas de Relatório, para que você possa definir as características do agendamento do novo relatório.
10. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, talvez você queira equilibrar os pares de HA com base na capacidade do agregado.

Crie um relatório para visualizar os nós que executam versões antigas do ONTAP no Active IQ Unified Manager

Você pode criar um relatório para exibir a versão do software ONTAP instalada em todos os nós do cluster, permitindo identificar quais nós devem ser atualizados.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada que exiba os nós que executam versões mais antigas do ONTAP e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Nós**.
2. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não queira no relatório.
3. Arraste a coluna “OS Version” para perto da coluna “Node”.
4. Clique na parte superior da coluna “OS Version” para classificar os resultados pela versão mais antiga do ONTAP.
5. Salve a visualização com um nome específico que reflita o que ela está mostrando, por exemplo, “Nós por versão do ONTAP”.
6. Clique no botão **Relatórios Agendados** na página de inventário.
7. Clique em **Adicionar Cronograma** para adicionar uma nova linha à página Cronogramas de Relatório, para que você possa definir as características do agendamento do novo relatório.
8. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, talvez seja interessante atualizar os nós que executam versões mais antigas do ONTAP.

Personalize os relatórios de capacidade do agregado

Crie um relatório para visualizar os agregados que atingiram a capacidade máxima no Active IQ Unified Manager

Você pode criar um relatório para encontrar os agregados que estão atingindo a capacidade máxima para que possa adicionar mais capacidade ou mover cargas de trabalho para outros agregados.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos a seguir para criar uma visualização personalizada que mostre os agregados atingindo a capacidade total e, em seguida, agende a geração de um relatório para essa visualização.

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 as colunas que você não quer no relatório.
4. Clique no ícone de filtro, adicione o seguinte filtro e, em seguida, clique em **Apply Filter**:
   - Menos de 45 dias até a capacidade total
5. Clique na parte superior da coluna “Days to Full” 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 total do agregado”, e clique na marca de seleção (✓).
7. Clique no botão **Relatórios Agendados** na página de inventário.
8. Clique em **Add Schedule** para adicionar uma nova linha à página **Report Schedules**, para que você possa definir as características do agendamento para o novo relatório.
9. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, talvez você queira aumentar o armazenamento nos agregados que estão atingindo a capacidade máxima. Além disso, talvez você queira aumentar o limite de "Dias até a capacidade máxima" para mais de 7 dias, que é o padrão, para receber eventos que deem mais tempo para reagir à falta de espaço nos agregados.

Crie um relatório para visualizar agregados que estejam com 80% ou mais de sua capacidade preenchida no Active IQ Unified Manager

Você pode criar um relatório para destacar os agregados que estão com 80% ou mais de sua capacidade preenchida.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para criar uma visualização personalizada que mostre agregados com 80% ou mais

de ocupação e, em seguida, agende a geração de um relatório para essa visualização.

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 as colunas que você não quer no relatório.
4. Arraste as colunas “Available Data %” e “Used Data %” para perto da coluna “Aggregate”.
5. Clique no ícone de filtro, adicione os seguintes filtros e, em seguida, clique em **Apply Filter**:
   - A porcentagem de dados utilizados é superior a 80%
6. Clique na parte superior da coluna “Used Data %” 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 próximos da capacidade total”, e clique na marca de seleção (✓) .
8. Clique no botão **Relatórios Agendados** na página de inventário.
9. Clique em **Adicionar Cronograma** para adicionar uma nova linha à página Cronogramas de Relatório, para que você possa definir as características do agendamento do novo relatório.
10. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, talvez você queira mover alguns dados de determinados agregados.

Crie um relatório para visualizar os agregados que estão sobrecarregados no Active IQ Unified Manager

Você pode criar um relatório para analisar a capacidade de storage e o uso de agregados, bem como visualizar os agregados que estão superalocados.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para criar uma visualização personalizada que exiba agregados que estão excedendo o limite de superalocação e, em seguida, agende a geração de um relatório para essa visualização.

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 queira no relatório.
4. Arraste a coluna “Overcommitted Capacity %” para perto da coluna “Aggregate”.
5. Clique no ícone de filtro, adicione os seguintes filtros e, em seguida, clique em **Apply Filter**:
   - A porcentagem de capacidade supercomprometida é superior a 100%
6. Clique no topo da coluna “Capacidade sobrecarregada %” 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 sobrecarregados”, e clique na marca de seleção (✓).
8. Clique no botão **Relatórios Agendados** na página de inventário.
9. Clique em **Adicionar Cronograma** para adicionar uma nova linha à página Cronogramas de Relatório, para que você possa definir as características do agendamento do novo relatório.
10. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados mostrados no relatório, você talvez queira adicionar mais capacidade aos agregados ou mover alguns dados de determinados agregados.

Personalize os relatórios de capacidade de volume

Identifique volumes próximos da capacidade máxima com o Snapshot Autodelete desativado no Active IQ Unified Manager

Você pode criar um relatório que contenha a lista de volumes que estão se aproximando da capacidade máxima com o Snapshot Autodelete desativado. Os resultados podem ajudar a identificar volumes nos quais você pode querer configurar o Snapshot Autodelete.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada que exiba as colunas necessárias na ordem correta e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Capacidade** > **Todos os volumes**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que você não quer no relatório.
4. Arraste e solte as colunas “Snapshot Autodelete” e “Days To Full” próximas à coluna “Available Data Capacity”.
5. Clique no ícone de filtro, adicione os dois filtros a seguir e clique em **Aplicar filtro**:
   - Dias até ficar cheio em menos de 30 dias
   - O Snapshot Autodelete está desativado
6. Clique na parte superior da coluna **Dias até ficar cheio** 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 ela está mostrando, por exemplo “Vols near capacity”.
8. Clique no botão **Relatórios Agendados** na página de inventário.
9. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode ativar a Snapshot Autodelete nos volumes ou encontrar uma maneira de aumentar o espaço disponível.

Identifique os volumes com thin provisioning desativado no Active IQ Unified Manager

Quando um volume não usa thin provisioning, ele ocupa todo o espaço em disco definido no momento da sua criação. Identificar os volumes com thin provisioning desativado ajuda você a decidir se deseja ativar esse recurso em determinados volumes.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada que exiba as colunas necessárias na ordem correta e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Capacidade** > **Todos os volumes**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que você não quer no relatório.
4. Arraste e solte as colunas “Used Data %” e “Thin Provisioned” próximas à coluna “Available Data Capacity”.
5. Clique no ícone de filtro, adicione o seguinte filtro, **Com thin provisioning** é **Não**, e clique em **Aplicar filtro**.
6. Clique na parte superior da coluna “Used Data %” para classificar os resultados de forma que os volumes com a maior porcentagem apareçam no topo da lista.
7. Salve a visualização com um nome que reflita o que ela está exibindo, 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 relatório**, para que você possa definir as características do agendamento para o novo relatório.
10. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode querer ativar thin provisioning em determinados volumes.

Identifique os volumes que devem mover dados para a camada de nuvem no Active IQ Unified Manager

Você pode criar um relatório que contenha a lista de volumes que atualmente residem em agregados FabricPool, que têm uma recomendação de nuvem de Tier e que contêm uma grande quantidade de dados frios. Este relatório pode ajudar você a decidir se deve alterar a política de disposição em camadas de determinados volumes para “auto” ou

“all” para descarregar mais dados frios (inativos) para a camada de nuvem.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado os agregados do FabricPool e ter volumes nesses agregados.

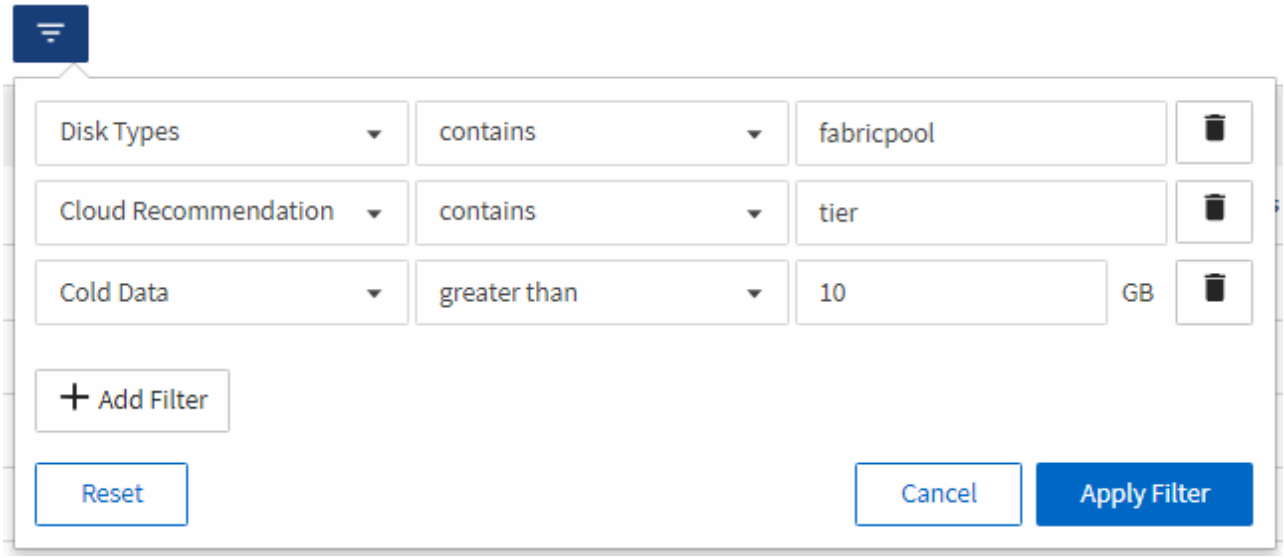
Siga os passos abaixo para criar uma visualização personalizada que exiba as colunas necessárias na ordem correta e, em seguida, agende a geração de um relatório para essa visualização.

Passos

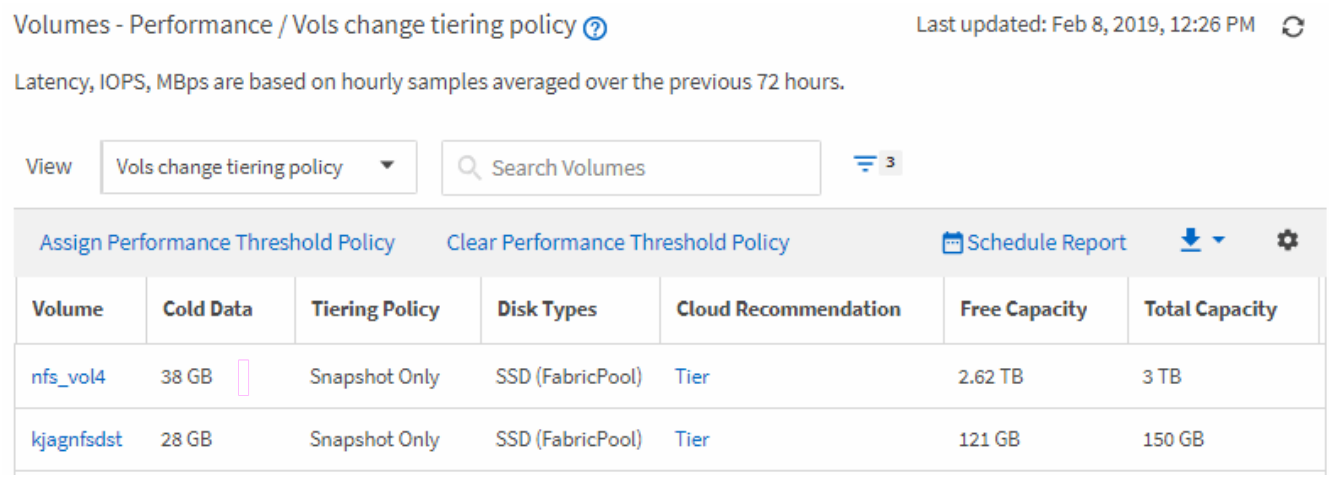
1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Desempenho** > **Todos os volumes**.
3. No seletor de colunas, certifique-se de que a coluna “Tipo de disco” apareça na visualização.

   Adicione ou remova outras colunas para criar uma visualização que seja importante para seu relatório.

4. Arraste e solte a coluna “Disk Type” próxima à coluna “Cloud Recommendation”.
5. Clique no ícone de filtro, adicione os três filtros a seguir e clique em **Aplicar filtro**:
   - O tipo de disco contém o FabricPool
   - A recomendação de nuvem contém nível
   - Dados frios maiores que 10 GB



6. Clique na parte superior da coluna "Dados Frios" para que os volumes com mais dados frios apareçam na parte superior da visualização.
7. Salve a visualização com um nome que reflita o que ela está mostrando, por exemplo “alterar política de tiering de
   volumes”.



8. Clique no botão **Relatórios Agendados** na página de inventário.
9. Clique em **Adicionar Cronograma** para adicionar uma nova linha à página Cronogramas de Relatório, para que você possa definir as características do agendamento do novo relatório.
10. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados mostrados no relatório, você pode usar o System Manager ou a ONTAP CLI para alterar a política de armazenamento em camadas para “auto” ou “all” em determinados volumes, a fim de descarregar mais dados frios para a camada de nuvem.

Personalize os relatórios de capacidade do Qtree

Crie um relatório para visualizar as qtrees que estão quase cheias no Active IQ Unified Manager

Você pode criar um relatório para analisar a capacidade de storage e a utilização de qtrees, bem como visualizar qtrees que estão quase cheias.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada que mostre as qtrees que estão quase cheias e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Qtrees**.
2. Selecione **Mostrar/Ocultar** para remover as colunas que você não quer no relatório.
3. Arraste a coluna “Disk Used %” para perto da coluna “Qtrees”.
4. Clique no ícone de filtro, adicione os seguintes filtros e, em seguida, clique em **Apply Filter**:
   - A porcentagem de uso do disco é superior a 75%
5. Clique no topo da coluna “Disk Used %” para classificar os resultados por porcentagem da capacidade.
6. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo, “Qtrees quase cheios”, 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 relatório**, para que você possa definir as características do agendamento para o novo relatório.
9. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, talvez seja necessário ajustar os limites rígidos e flexíveis de disco (se definidos) ou equilibrar os dados entre as qtrees.

Personalize relatórios de compartilhamento NFS

Personalize os relatórios de compartilhamento NFS no Active IQ Unified Manager

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 os volumes que possuem um caminho de montagem inacessível no Active IQ Unified Manager

Você pode criar um relatório para encontrar volumes que tenham um caminho de montagem inacessível.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para criar uma visualização personalizada para volumes que têm um caminho de montagem inacessível e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Compartilhamentos NFS**.
2. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não queira no relatório.
3. Clique no ícone de filtro, adicione o seguinte filtro e, em seguida, clique em **Apply Filter**:
   - O caminho de montagem ativo é Não
4. Salve a visualização com um nome específico que reflita o que a visualização mostra, 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 relatório, para que você possa definir as características do agendamento do novo relatório.
7. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail

aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, talvez você queira corrigir os caminhos de montagem inacessíveis.

Crie um relatório para visualizar volumes usando a política de exportação padrão no Active IQ Unified Manager

Você pode criar um relatório para encontrar volumes que estejam usando a política de exportação padrão.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada para volumes que utilizam a política de exportação padrão e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Compartilhamentos NFS**.
2. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não queira no relatório.
3. Arraste a coluna “Export Policy” para perto da coluna “Volume”.
4. Clique no ícone de filtro, adicione o seguinte filtro e, em seguida, clique em **Apply Filter**:
   - A política de exportação contém o padrão
5. Salve a visualização com um nome específico que reflita o que a visualização 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 relatório, para que você possa definir as características do agendamento do novo relatório.
8. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados mostrados no relatório, você talvez queira configurar uma política de exportação personalizada.

Personalize os relatórios de VMs de armazenamento

Personalize os relatórios de máquinas virtuais de armazenamento no Active IQ Unified Manager

Você pode criar relatórios de máquinas virtuais de storage (SVMs) para analisar informações de volume e visualizar a integridade geral e a disponibilidade de storage. Por exemplo, você pode criar relatórios para exibir as SVMs que atingiram a contagem máxima de volume e para analisar as SVMs interrompidas.

Crie um relatório para visualizar as VMs de armazenamento que estão atingindo o limite máximo de volumes no Active IQ Unified Manager

Você pode criar um relatório para encontrar SVMs que estão atingindo o limite máximo de volume.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para criar uma visualização personalizada que mostre as VMs de storage que estão atingindo o limite máximo de volume e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **VMs de armazenamento**.
2. Selecione **Mostrar/Ocultar** para remover as colunas que você não quer no relatório.
3. Arraste as colunas “Volume Count” e “Maximum Allowed Volumes” para perto da coluna “Storage VM”.
4. Clique na parte superior da coluna “Volumes Máximos Permitidos” para classificar os resultados pelo maior número de volumes.
5. Salve a 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 **Add Schedule** para adicionar uma nova linha à página **Report Schedules**, para que você possa definir as características do agendamento para o novo relatório.
8. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode querer equilibrar os volumes atribuídos às VMs de storage ou, se possível, usar o ONTAP System Manager para alterar o número máximo de volumes permitidos.

Crie um relatório para visualizar as VMs de armazenamento interrompidas no Active IQ Unified Manager

Você pode criar um relatório para exibir uma lista de todas as SVMs paradas.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada que mostre as VMs de storage paradas e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **VMs de armazenamento**.
2. No menu Exibir, selecione **Saúde** > **Todas as VMs de storage**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não queira no relatório.
4. Arraste a coluna “State” para perto da coluna “Storage VM”.

5. Clique no ícone de filtro, adicione o seguinte filtro e, em seguida, clique em **Apply Filter**:
   - O estado está parado
6. Salve a visualização com um nome específico que reflita o que a visualização está mostrando, por exemplo “SVMs parados” e clique na marca de seleção (✓).
7. Clique no botão **Relatórios Agendados** na página de inventário.
8. Clique em **Add Schedule** para adicionar uma nova linha à página **Report Schedules**, para que você possa definir as características do agendamento para o novo relatório.
9. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, talvez você queira investigar por que a SVM está parada para verificar se deve reiniciar as SVMs paradas.

Personalize os relatórios de relacionamento de volume

Personalize os relatórios de relacionamento de volume no Active IQ Unified Manager

O relatório de inventário de relacionamentos de volume permite que você analise os detalhes do inventário de storage em um cluster, entenda o grau de proteção necessário para os volumes e filtre os detalhes dos volumes com base na origem da falha, no padrão e nos agendamentos.

Crie um relatório para agrupar as relações de volume por origem da falha no Active IQ Unified Manager

Você pode criar um relatório que agrupa os volumes de acordo com o motivo pelo qual o relacionamento está em um estado não íntegro.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada que agrupe os volumes por origem da falha e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Relacionamento** > **Todos os Relacionamentos**.
3. Selecione **Mostrar/Ocultar** para garantir que as colunas “Relationship Health” e “Unhealthy Reason” apareçam na visualização.

   Adicione ou remova outras colunas para criar uma visualização que seja importante para seu relatório.
4. Arraste as colunas “Relationship Health” e “Unhealthy Reason” para perto da coluna “State”.
5. Clique no ícone de filtro, adicione o seguinte filtro e, em seguida, clique em **Apply Filter**:
   - A saúde do relacionamento é ruim
6. Clique na parte superior da coluna “Unhealthy Reason” para agrupar as relações de volume por origem da

falha.

7. Salve a visualização com um nome específico que reflita o que ela está mostrando, por exemplo, “Relações de vol. por falha”.
8. Clique no botão **Relatórios Agendados** na página de inventário.
9. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode investigar a origem e o impacto de cada tipo de falha.

Crie um relatório para agrupar as relações de volume por problema no Active IQ Unified Manager

Você pode criar um relatório que agrupe as relações de volume por problema.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada que agrupe as relações de volume por problema e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Relacionamento** > **Todos os Relacionamentos**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que você não quer no relatório.
4. Arraste a coluna “Unhealthy Reason” para perto da coluna “State”.
5. Clique na parte superior da coluna “Motivo não íntegro” para agrupar os volumes por problema.
6. Salve a visualização com um nome específico que reflita o que ela está mostrando, por exemplo, “Relações de volume por problema”.
7. Clique no botão **Relatórios Agendados** na página de inventário.
8. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode investigar a origem e o impacto de cada tipo de problema.

Crie um relatório para visualizar as tendências de transferência de volume em intervalos de tempo no Active IQ Unified Manager

Você pode criar um relatório que exibe as tendências de transferência de volume em intervalos de tempo específicos.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para criar uma visualização personalizada para volumes em intervalos de tempo específicos e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu View, selecione **Relationship** > **Last 1 month Transfer Status**.
3. Selecione **Mostrar/Ocultar** para remover as colunas que você não quer no relatório.
4. Arraste a coluna "Transfer Duration" para perto da coluna “Operational Result”.
5. Clique no ícone de filtro, adicione o seguinte filtro e, em seguida, clique em **Apply Filter**:
   - 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 ela está exibindo, por exemplo, “Volumes por duração”.
8. Clique no botão **Relatórios Agendados** na página de inventário.
9. Insira um nome para o cronograma do relatório, defina a frequência como **Semanal** e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode investigar os intervalos de tempo de transferência.

Crie um relatório para visualizar as transferências de volume com falha ou bem-sucedidas no Active IQ Unified Manager

Você pode criar um relatório que exibe o status das transferências de volume. Nesse relatório, você pode visualizar tanto as transferências de volume com falha quanto as bem-sucedidas.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada que mostre quais transferências falharam e quais foram bem-sucedidas e em seguida agende um relatório para essa visualização.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu View, selecione **Relationship** > **Last 1 month Transfer Status**.
3. Selecione **Mostrar/Ocultar** para remover quaisquer colunas que você não queira no relatório.
4. Arraste a coluna “Resultado da Operação” para perto da coluna “Estado”.
5. Clique na parte superior da coluna “Operation Result” para classificar os volumes pelo status.
6. Salve a visualização com um nome específico que reflita o que ela está exibindo, por exemplo “Volumes por status de transferência”.
7. Clique no botão **Relatórios Agendados** na página de inventário.

8. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode investigar o status da transferência.

Crie um relatório para visualizar as transferências de volume com base no tamanho da transferência no Active IQ Unified Manager

Você pode criar um relatório para visualizar as transferências de volume com base no tamanho da transferência.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para criar uma visualização personalizada para transferências de volume com base no tamanho da transferência e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Relacionamento** > **Taxa de transferência do último mês**.
3. Clique na parte superior da coluna “Total Transfer Size” para classificar as transferências de volumes por tamanho.
4. Salve a visualização com um nome específico que reflita o que ela está exibindo, por exemplo “Volumes por tamanho de transferência”.
5. Clique no botão **Relatórios Agendados** na página de inventário.
6. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode investigar as relações de volume por tamanho de transferência.

Crie um relatório para visualizar as transferências de volume agrupadas por dia no Active IQ Unified Manager

Você pode criar um relatório para visualizar as transferências de volume agrupadas por dia.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga os passos abaixo para criar uma visualização personalizada das transferências de volume agrupadas por dia e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.

2. No menu Exibir, selecione **Relacionamento** > **Taxa de transferência do último mês**.
3. Clique na parte superior da coluna “Day” para classificar as transferências de volume por dia.
4. Salve a visualização com um nome específico que reflita o que ela está mostrando, por exemplo “Transferências de volume por dia”.
5. Clique no botão **Relatórios Agendados** na página de inventário.
6. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

   O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode analisar as transferências de volume por dia.

Personalize os relatórios de desempenho de volume

Crie um relatório para identificar volumes com alta concentração de dados frios em um agregado que não seja o FabricPool no Active IQ Unified Manager

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 do FabricPool.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para criar uma visualização personalizada para volumes com uma grande quantidade de dados inativos em um agregado não habilitado para o FabricPool e, em seguida, agende a geração de um relatório para essa visualização.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Desempenho** > **Todos os volumes**.
3. Selecione **Mostrar/Ocultar** para garantir que a coluna “Disk Type” apareça na visualização.

   Adicione ou remova outras colunas para criar uma visualização que seja 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, em seguida, clique em **Apply Filter**:
   - Dados frios com mais de 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 ela está exibindo, por exemplo “Volumes de dados frios não FabricPool”.
8. Clique no botão **Relatórios Agendados** na página de inventário.
9. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode encontrar volumes que são bons candidatos para serem movidos para agregados do FabricPool.

Exemplos de relatórios do Microsoft Excel

Entenda exemplos de relatórios do Microsoft Excel no Active IQ Unified Manager

Estes exemplos de relatórios do Microsoft Excel têm como objetivo apresentar as opções de geração de relatórios disponíveis usando os recursos avançados do Excel.

As funcionalidades avançadas do Excel permitem criar uma ampla variedade de relatórios específicos para as suas necessidades. Para obter informações completas sobre como usar o Excel, consulte a documentação do produto.

Você precisa ter a função de Application Administrator ou Storage Administrator para gerenciar relatórios.

Crie um relatório para exibir uma tabela e um gráfico de capacidade agregada no Active IQ Unified Manager

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 precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para abrir uma visualização de Saúde: todos os agregados, baixar a visualização em 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 **Reports** > **Download Excel**.



Dependendo do seu navegador, talvez seja necessário clicar em **OK** para salvar o arquivo.

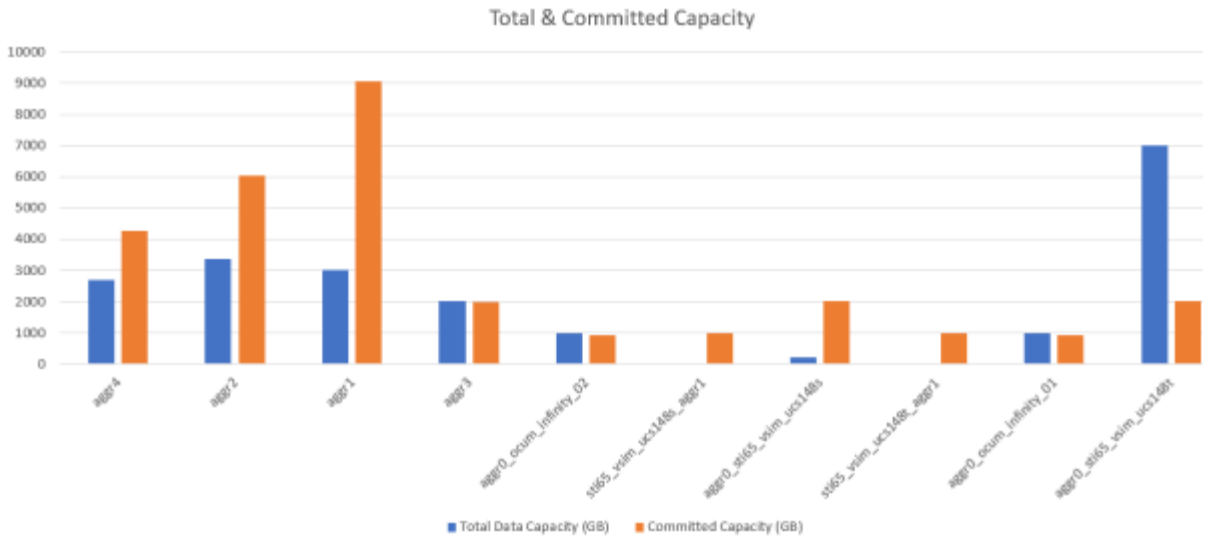
3. Se necessário, clique em **Enable Editing**.
4. No Excel, abra o arquivo baixado.
5. Crie uma nova planilha (⊕) após a `data` planilha e nomeie-a como **Capacidade Total de Dados**.
6. Adicione as seguintes colunas na nova planilha Total Data Capacity:
   a. Capacidade total de dados (GB)
   b. Capacidade comprometida (GB)
   c. Capacidade de dados utilizada (GB)
   d. Capacidade de dados disponível (GB)
7. Na primeira linha de cada coluna, insira a seguinte fórmula, certificando-se de que ela faça referência à datasheet (data!) e aos especificadores corretos de coluna e linha para os dados capturados (a capacidade total de dados extrai dados da coluna E, das linhas 2 a 20).

   a. =SOMA(data!E$2:data!E$20)
   b. =SUM(data!F$2:data!F$50)
   c. =SOMA(data!G$2:data!G$50)
   d. =SOMA(data!H$2:data!H$50)

   A fórmula totaliza cada coluna com base nos dados atuais.

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. Na datasheet, selecione as colunas **Capacidade total de dados (GB)** e **Capacidade comprometida (GB)**.
2. Selecione **Gráficos Recomendados** no menu **Inserir** e selecione o gráfico de **Colunas Agrupadas**.
3. Clique com o botão direito do mouse no gráfico e selecione **Mover gráfico** para movê-lo para a `Total Data Capacity` planilha.
4. Usando os menus **Design** e **Format**, que estão disponíveis quando o gráfico está selecionado, você pode personalizar a aparência do gráfico.
5. Quando estiver satisfeito, salve o arquivo com suas alterações. Não altere o nome ou a localização do arquivo.

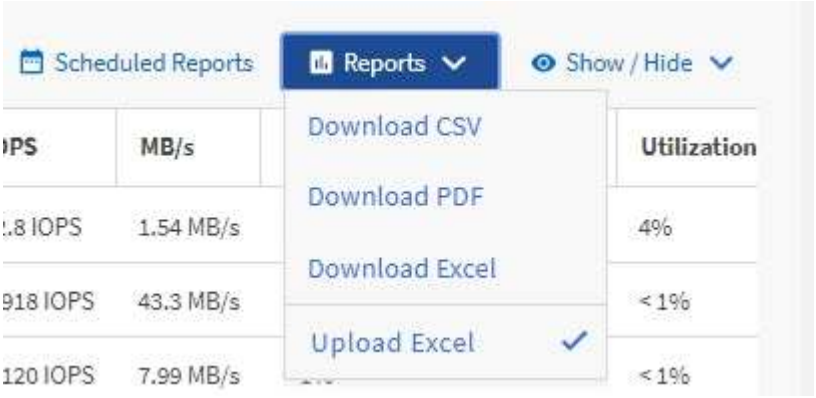


6. No Unified Manager, selecione **Reports** > **Upload Excel**.

   Certifique-se de estar na mesma visualização em que você baixou o arquivo do Excel.

7. Selecione o arquivo Excel que você modificou.
8. Clique em **Abrir**.
9. Clique em **Enviar**.

   Uma marca de seleção aparece ao lado do item de menu **Reports** > **Upload Excel**.



10. Clique em **Relatórios Agendados**.
11. Clique em **Adicionar Cronograma** para adicionar uma nova linha à página Cronogramas de Relatório, para que você possa definir as características do agendamento do novo relatório.

    Selecione o formato **XLSX** para o relatório.

12. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados mostrados no relatório, talvez você queira investigar a melhor forma de usar a

capacidade disponível em toda a sua rede.

Exibir gráficos de capacidade total agregada versus capacidade disponível no Active IQ Unified Manager

Você pode criar um relatório para analisar a capacidade total de storage e a capacidade comprometida em um formato de gráfico do Excel.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para abrir uma visualização Health: All Aggregates, baixar a visualização no Excel, criar um gráfico de capacidade total e comprometida, carregar o arquivo personalizado do Excel e agendar o relatório final.

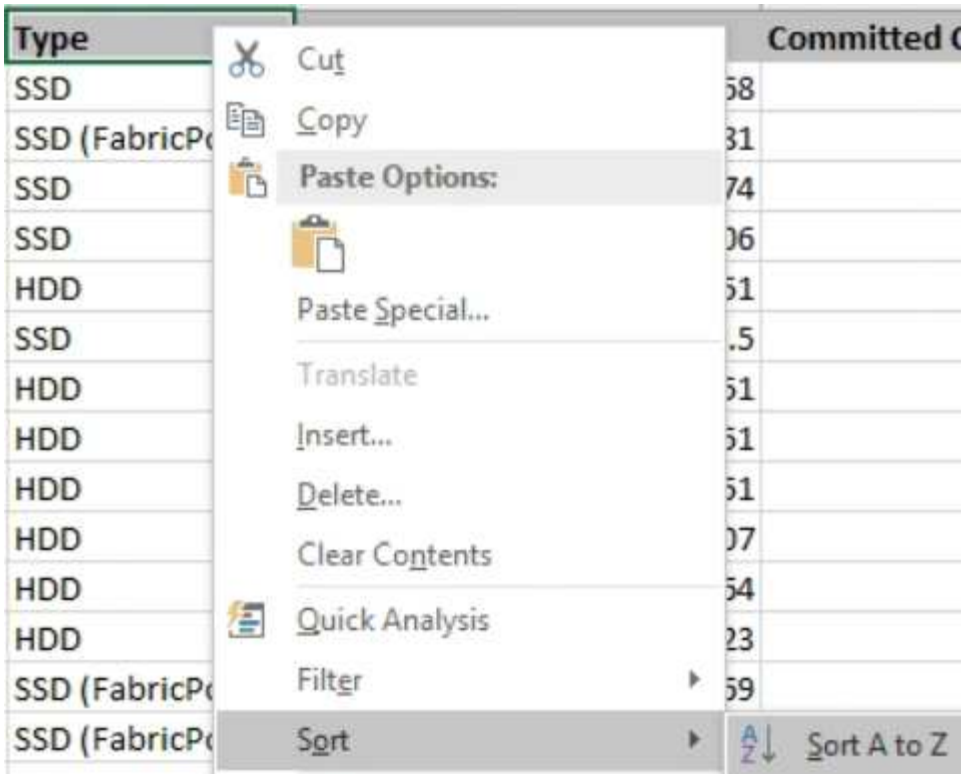
Passos

1. No painel de navegação esquerdo, clique em **Armazenamento** > **Agregados**.
2. Selecione **Reports** > **Download Excel**.



   Dependendo do seu navegador, talvez seja necessário clicar em **OK** para salvar o arquivo.

3. No Excel, abra o arquivo baixado.
4. Se necessário, clique em **Enable Editing**.
5. Na datasheet, clique com o botão direito do mouse na coluna Type e selecione **Sort** > **Sort A to Z**.

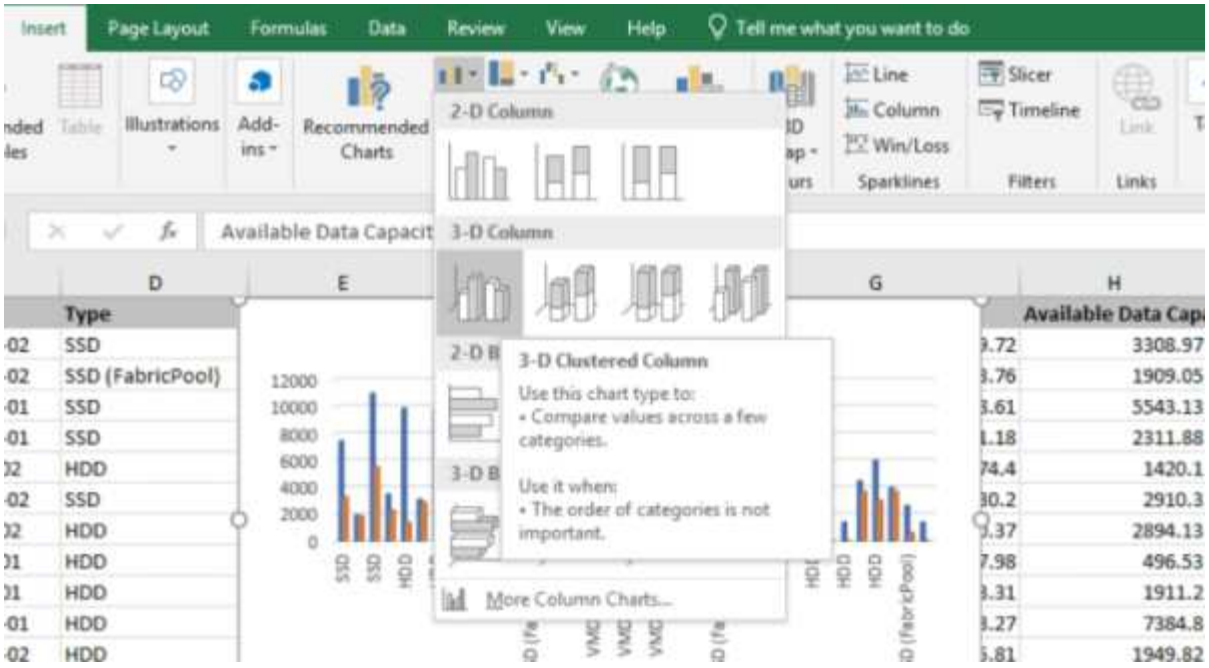


Isso organizará seus dados por tipo de armazenamento, como:

- HDD
- Híbrido
- SSD
- SSD (FabricPool)

6. Selecione as colunas `Type, Total Data Capacity,` e `Available Data Capacity`.
7. No menu **Inserir**, selecione um `3-D column` gráfico.

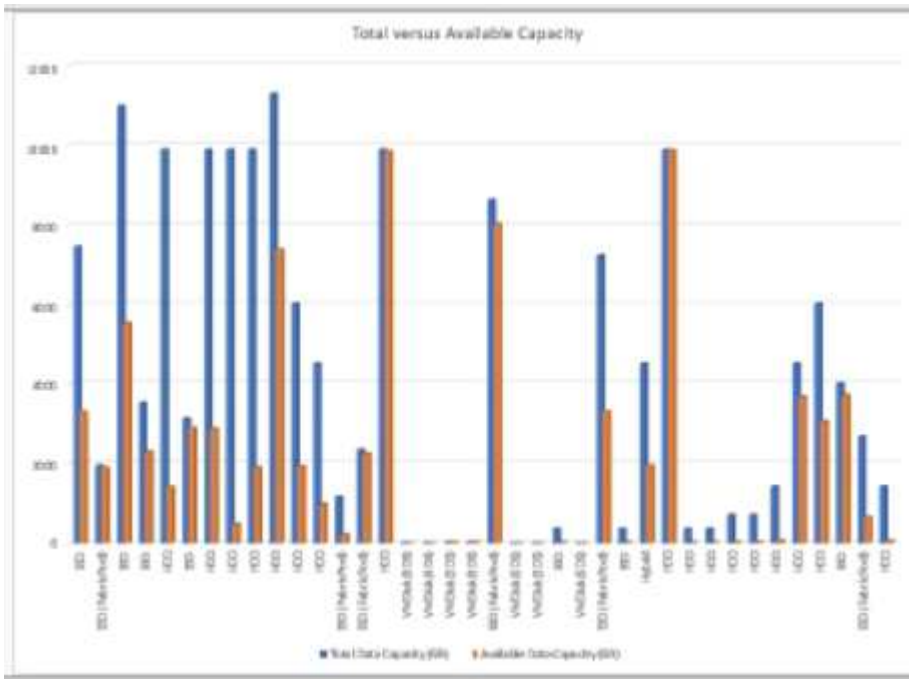
   O gráfico aparece na datasheet.



8. Clique com o botão direito do mouse no gráfico e selecione **Mover gráfico**.
9. Selecione **Nova planilha** e dê à planilha o nome de **Gráficos de armazenamento total**.

> Certifique-se de que a nova planilha apareça após as planilhas de informações e dados.

10. Dê ao gráfico o título **Capacidade Total versus Capacidade Disponível**.
11. Utilizando os menus **Design** e **Format**, disponíveis quando o gráfico está selecionado, você pode personalizar a aparência do gráfico.
12. Quando estiver satisfeito, salve o arquivo com suas alterações. Não altere o nome ou a localização do arquivo.

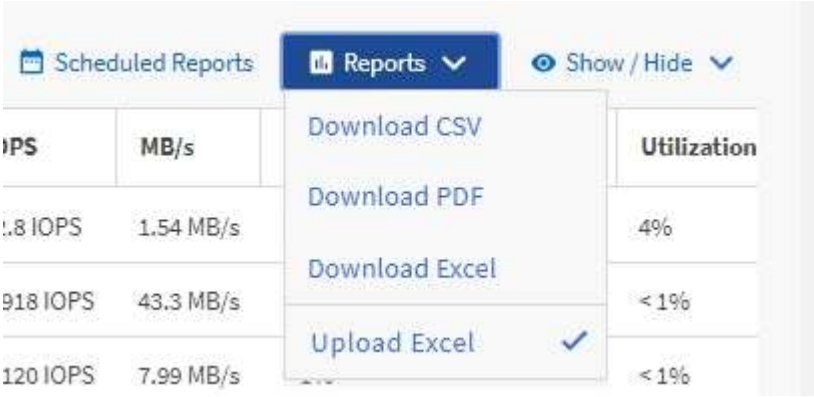


13. No Unified Manager, selecione **Reports** > **Upload Excel**.

Certifique-se de estar na mesma visualização em que você 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 **Reports** > **Upload Excel**.



17. Clique em **Relatórios Agendados**.
18. Clique em **Add Schedule** para adicionar uma nova linha à página **Report Schedules**, para que você possa definir as características do agendamento para o novo relatório.

    Selecione o formato **XLSX** para o relatório.

19. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, talvez seja interessante equilibrar a carga nos seus agregados.

Crie um relatório para visualizar gráficos de capacidade de volume disponível no Active IQ Unified Manager

Você pode criar um relatório para analisar a capacidade de volume disponível em um gráfico do Excel.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para abrir uma visualização de Saúde: todos os Volumes, baixar a visualização no Excel, criar um gráfico de capacidade disponível, carregar o arquivo do Excel personalizado e agendar o relatório final.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.

2. Selecione **Reports** > **Download Excel**.



   Dependendo do seu navegador, talvez seja necessário clicar em **OK** para salvar o arquivo.

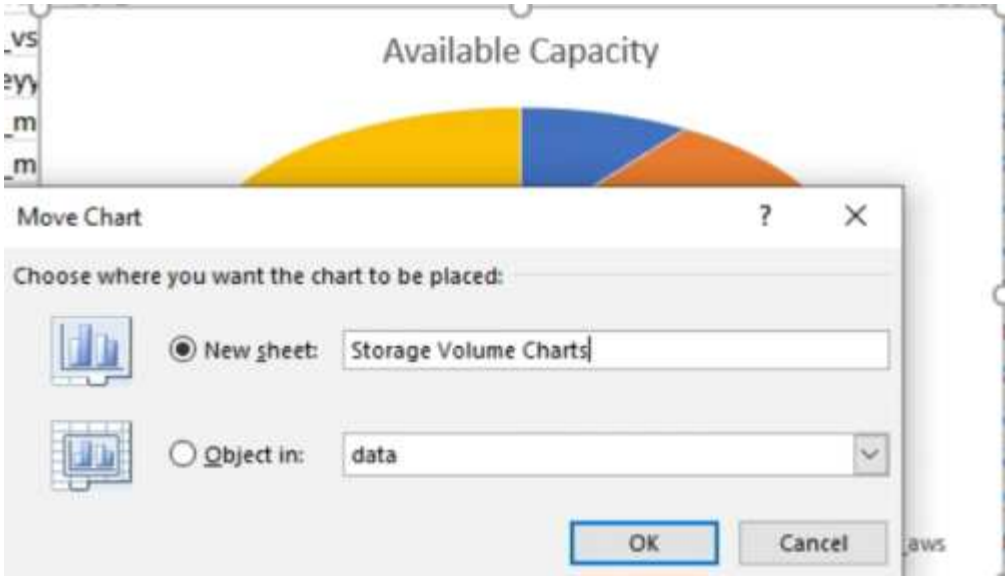
3. Se necessário, clique em **Enable Editing**.
4. No Excel, abra o arquivo baixado.
5. Na `data` planilha, selecione os dados que deseja usar nas colunas `Volume` e `Available Data` %.
6. No menu **Inserir**, selecione um `3-D piechart.`

   O gráfico mostra quais volumes têm o maior espaço disponível. O gráfico aparece na datasheet.

   > Dependendo da configuração da sua rede, selecionar colunas inteiras ou muitas linhas de dados pode tornar o 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 represente os dados que você deseja capturar.

7. Dê ao gráfico o título **Available Capacity**.
8. Clique com o botão direito do mouse no gráfico e selecione **Mover gráfico**.
9. Selecione **Nova planilha** e nomeie a planilha como **Storage Volume Charts**.

   > Certifique-se de que a nova planilha apareça após as planilhas de informações e dados.

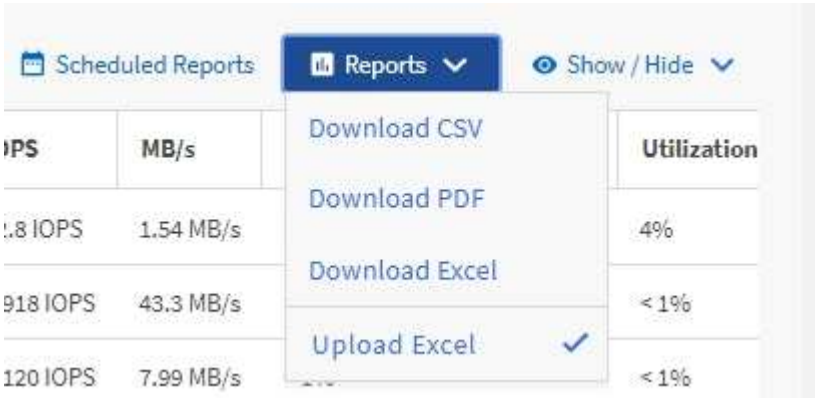


10. Utilizando os menus **Design** e **Format**, disponíveis quando o gráfico está selecionado, você pode personalizar a aparência do gráfico.
11. Quando estiver satisfeito, salve o arquivo com suas alterações.
12. No Unified Manager, selecione **Reports** > **Upload Excel**.

    Certifique-se de estar na mesma visualização em que você 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 **Reports** > **Upload Excel**.



16. Clique em **Relatórios Agendados**.
17. Clique em **Add Schedule** para adicionar uma nova linha à página **Report Schedules**, para que você possa definir as características do agendamento para o novo relatório.
18. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    Selecione o formato **XLSX** para o relatório.

O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, talvez seja interessante equilibrar a carga nos seus volumes.

Crie um relatório para visualizar os agregados com o maior número de IOPS disponíveis no Active IQ Unified Manager

Este relatório mostra quais agregados têm o maior número de IOPS disponíveis por tipo de agregado em que você pode provisionar novas cargas de trabalho.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.

Siga as etapas a seguir para abrir uma visualização de Saúde: todos os Volumes, baixar a visualização no Excel, criar um gráfico de capacidade disponível, carregar o arquivo do 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 a coluna `Available IOPS` e ocultar as colunas `Cluster FQDN`, `Inactive Data Reporting`, e `Threshold Policy`.
4. Arraste e solte as colunas `Available IOPS` e `Free Capacity` ao lado da coluna `Type`.
5. Dê um nome e salve a visualização personalizada `Available IOPS Per Aggr`.
6. Selecione **Reports** > **Download Excel**.



   Dependendo do seu navegador, talvez seja necessário clicar em **OK** para salvar o arquivo.

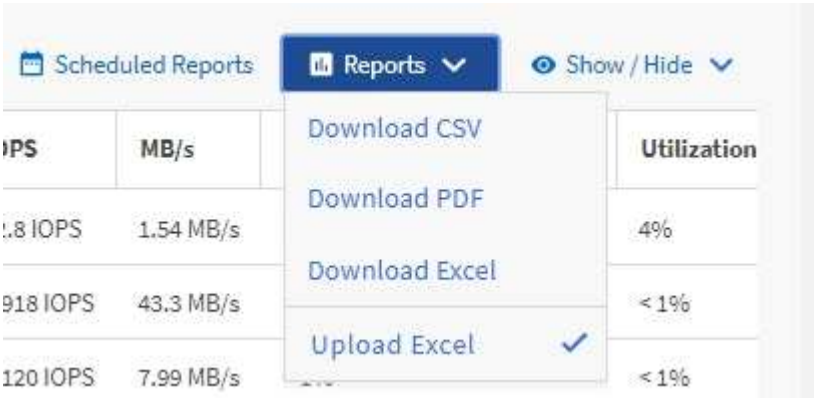
7. Se necessário, clique em **Enable Editing**.
8. No Excel, abra o arquivo baixado.
9. Na datasheet, clique no pequeno triângulo no canto superior esquerdo da planilha para selecionar a planilha inteira.

10. Na faixa de opções **Dados**, selecione **Classificar** na `Sort & Filter area.`
11. Defina os seguintes níveis de classificação:
    a. Especifique **Sort by** como `Available IOPS` (IOPS), **Sort On** como `Cell Values,` e **Order** como `Largest to Smallest.`
    b. Clique em **Adicionar nível**.
    c. Especifique **Classificar por** como `Type`, **Classificar em** como `Cell Values,` e **Ordem** como `Z to A.`
    d. Clique em **Adicionar nível**.
    e. Especifique **Classificar por** como `Free Capacity (GB),` **Classificar em** como `Cell Values,` e **Ordem** como `Largest to Smallest.`
    f. Clique em **OK**.
12. Salve e feche o arquivo do Excel.
13. No Unified Manager, selecione **Reports** > **Upload Excel**.

    Certifique-se de estar na mesma visualização em que você baixou o arquivo do Excel.

14. Selecione o arquivo do 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 **Reports** > **Upload Excel**.



17. Clique em **Relatórios Agendados**.
18. Clique em **Adicionar Cronograma** para adicionar uma nova linha à página Cronogramas de Relatório, para que você possa definir as características do agendamento do novo relatório.
19. Insira um nome para o cronograma do relatório e preencha os outros campos do relatório, depois clique na marca de seleção (✓) no final da linha.

    Selecione o formato **XLSX** para o relatório.

    O relatório é enviado imediatamente como teste. Depois disso, o relatório é gerado e enviado por e-mail aos destinatários listados na frequência especificada.

Com base nos resultados apresentados no relatório, você pode querer provisionar novas cargas de trabalho nos agregados que possuem o maior número de IOPS disponíveis.

Gerencie o armazenamento usando APIs REST

Primeiros passos com Active IQ Unified Manager

Comece a usar as APIs REST do Active IQ Unified Manager

O Active IQ Unified Manager fornece um conjunto de APIs para gerenciar seus recursos de storage nos sistemas de armazenamento compatíveis por meio de uma interface de serviço web RESTful para qualquer integração de terceiros.

Nestes tópicos, você encontrará informações sobre as APIs do Unified Manager, fluxos de trabalho de exemplo para resolver problemas específicos e alguns códigos de exemplo. Com essas informações, você pode criar clientes RESTful de soluções de software de capacidade de gerenciamento da NetApp para gerenciar sistemas NetApp. As APIs são baseadas no estilo arquitetural Representational State Transfer (REST). Há suporte para todas as quatro operações REST: create, read, update e delete (também conhecidas como CRUD).

Consulte "Active IQ Unified Manager" para ver recursos adicionais e detalhes sobre os benefícios da API REST do Active IQ Unified Manager.

Identifique os usuários pretendidos das Active IQ Unified Manager REST APIs

Os tópicos apresentados aqui destinam-se a desenvolvedores que criam aplicativos que fazem interface com o software Active IQ Unified Manager por meio de APIs REST.

Administradores e arquitetos de storage podem consultar estas 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 storage NetApp.

Você deve usar essas informações se quiser usar as APIs de administração do provedor de armazenamento, do cluster ONTAP e de gerenciamento para gerenciar seu storage.

> Você deve ter uma das seguintes funções: Operador, Administrador de storage 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.

Gerencie o acesso à API e as categorias do Active IQ Unified Manager

As APIs do Active IQ Unified Manager permitem gerenciar e provisionar objetos de storage em seu ambiente. Você também pode acessar a interface web do Unified Manager para executar algumas dessas funções.

Crie 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://<hostname>/api

A porta padrão é 443. Você pode configurar a porta de acordo com as necessidades do seu ambiente.

Acesse a página de documentação da API online

Você pode acessar a página de conteúdo de referência da *Documentação da API*, incluída com o produto, para exibir a documentação da API, bem como para emitir manualmente uma chamada de API (na interface, por exemplo, o Swagger). Você pode acessar essa documentação ao clicar em **Barra de menu** > botão **Ajuda** > **Documentação da API**

Alternativamente, insira o nome do host ou o endereço IP e a URL para acessar a página da API REST no formato

https://<hostname>/docs/api/

Categorias

As chamadas da API são organizadas funcionalmente com base nas áreas ou categorias. Para localizar uma API específica, clique na categoria de API correspondente.

As APIs REST fornecidas com Unified Manager ajudam você a executar funções administrativas, de monitoramento e de provisionamento. As APIs estão agrupadas nas seguintes categorias.

- **data center**

  Esta categoria contém as APIs que ajudam você no gerenciamento de storage e nas análises do storage do data center usando ferramentas, como o Work Flow Automation e o Ansible. As APIs REST nesta categoria fornecem informações sobre os clusters, nós, agregados, volumes, LUNs, compartilhamentos de arquivos, namespaces e outros elementos no seu data center.

- **management-server**

  As APIs da categoria **management-server** contêm as APIs `jobs, system,` e `events`. Jobs são operações agendadas para execução assíncrona relacionadas ao gerenciamento de objetos de storage ou cargas de trabalho no Unified Manager. A API `events` retorna eventos no seu data center, e a API `system` retorna os detalhes da instância do Unified Manager.

- **storage-provider**

  Esta categoria contém todas as APIs de provisionamento necessárias para gerenciar e provisionar compartilhamentos de arquivos, LUNs, níveis de serviço de desempenho (PSLs) e políticas de eficiência de storage (SEPs). As APIs também permitem configurar endpoints de acesso, os Active Directories, bem como atribuir PSLs e SEPs às cargas de trabalho de storage.

- **administração**

  Esta categoria contém as APIs usadas para executar tarefas administrativas, como manter as configurações de backup, visualizar certificados do repositório confiável para as fontes de dados do Unified Manager e gerenciar clusters ONTAP como fontes de dados para o Unified Manager.

- **gateway**

  O Unified Manager permite que você invoque APIs REST do ONTAP por meio das APIs na categoria gateway e gerencie os objetos de storage em seu data center.

- **segurança**

  Esta categoria contém APIs para gerenciar usuários do Unified Manager.

Entenda os serviços REST oferecidos no Active IQ Unified Manager

É importante que você conheça os serviços e as operações REST oferecidos antes de começar a usar as APIs do Active IQ Unified Manager.

As APIs de provisionamento e administração usadas para configurar o servidor de API suportam operações de leitura (GET) ou gravação (POST, PATCH, DELETE). A seguir, alguns exemplos das operações GET, PATCH, POST e DELETE suportadas pelas APIs:

- Exemplo de GET: `GET /datacenter/cluster/clusters` recupera detalhes do cluster no seu data center. O número máximo de registros retornados pela `GET` operação é 1000.

  As APIs permitem filtrar, classificar e ordenar os registros por atributos suportados.

- Exemplo de POST: `POST /datacenter/svm/svms` cria uma Máquina Virtual de Armazenamento (SVM) personalizada.
- Exemplo de PATCH: `PATCH /datacenter/svm/svms/{key}` modifica as propriedades de uma SVM, usando sua chave única.
- Exemplo de DELETE: `DELETE /storage-provider/access-endpoints/{key}` exclui um endpoint 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 storage ou Administrador de aplicativos.

Função do usuário	Método REST suportado
Operador	Acesso somente leitura aos dados. Usuários com essa função podem executar todas as solicitações GET.
Administrador de storage	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 realizar atividades específicas, como gerenciar objetos do serviço de storage e opções de gerenciamento de storage.
Administrador de Aplicativos	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*.

Entenda os números de 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 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 anteriores em lançamentos futuros. Você também encontra as mesmas APIs sem uma versão, por exemplo `/datacenter/svm/svms,`, que indicam as APIs base sem uma versão. As APIs base são sempre a versão mais recente das APIs.

> No canto superior direito da sua 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 alta de uma determinada API, em relação ao 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 processar. Em solicitações REST, você deve incluir o parâmetro de versão. As versões anteriores das APIs acabam sendo descontinuadas após algumas versões. Nesta versão, a `v1` versão das APIs está descontinuada.

Entenda o modelo de recursos de armazenamento do ONTAP no Active IQ Unified Manager

Os recursos de storage no ONTAP podem ser amplamente classificados em *recursos de storage físico* e *recursos de storage lógico.* Para gerenciar seus sistemas ONTAP de forma eficaz usando as APIs fornecidas no Active IQ Unified Manager, você deve compreender o modelo de recursos de storage e a relação entre os vários recursos de storage.

- **Recursos de storage físico**

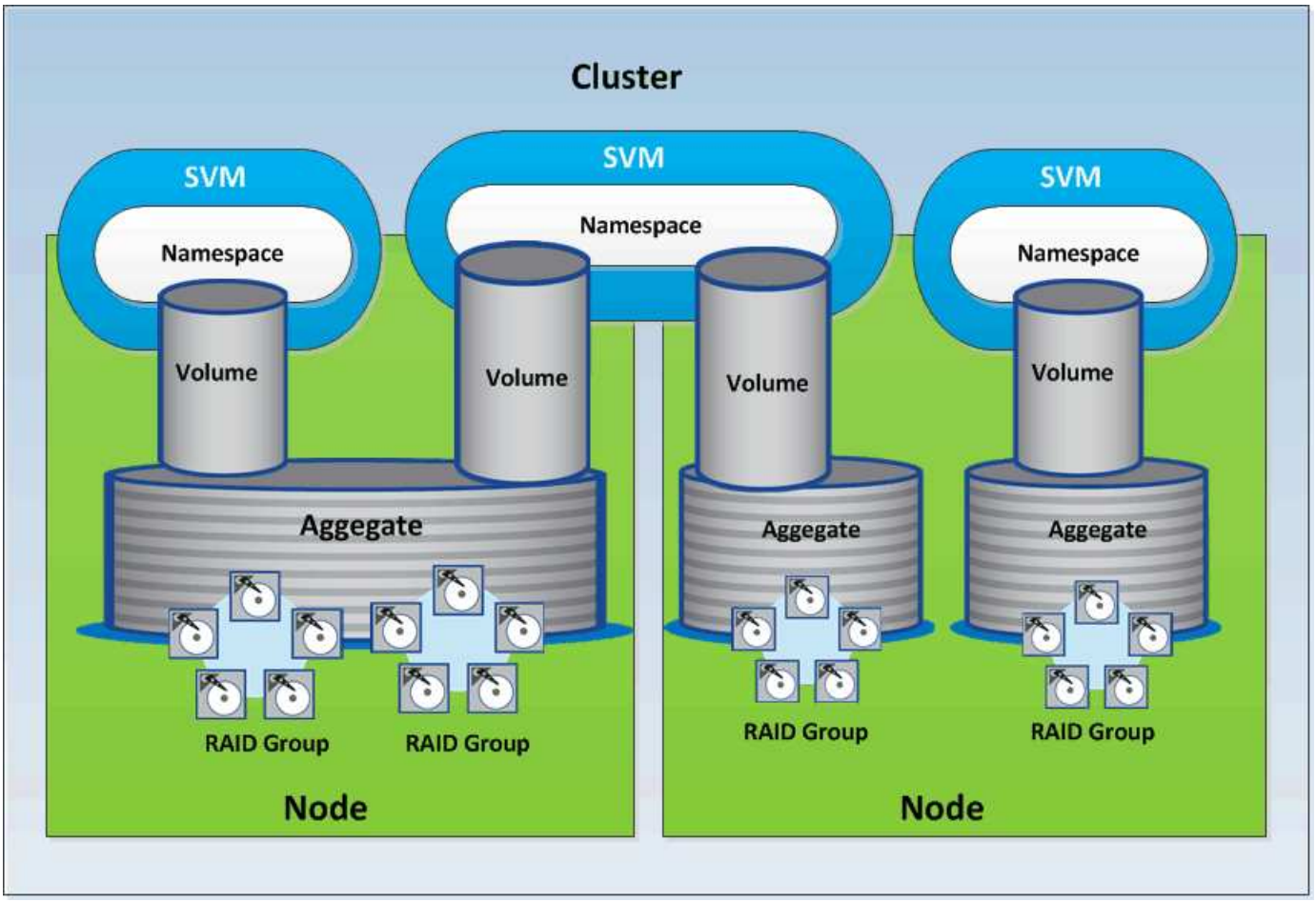
  Refere-se aos objetos de storage físico fornecidos pelo ONTAP. Os recursos de storage físico incluem discos, clusters, controladores de storage, nós e agregados.

- **Recursos lógicos de storage**

  Refere-se aos recursos de storage fornecidos pelo ONTAP que não estão vinculados a um recurso físico. Esses recursos estão associados a uma máquina virtual de storage (SVM, anteriormente conhecida como Vserver) e existem independentemente de qualquer recurso específico de storage físico, como um disco, uma LUN de array ou um agregado.

  Os recursos de storage lógico incluem volumes de todos os tipos e qtrees, bem como os recursos e as configurações que você pode usar com esses recursos, como cópias Snapshot, deduplicação, compactação e cotas.

A ilustração a seguir mostra os recursos de storage em um cluster de 2 nós:



Acesso à API REST e autenticação no Active IQ Unified Manager

Acesse e autentique APIs REST no Active IQ Unified Manager

A API REST do Active IQ Unified Manager pode ser acessada por meio de 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:

- **Solicitação**

```
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 da API.
- Porta 443

443 é a porta HTTPS padrão. Você pode personalizar a porta HTTPS, se necessário.
Para enviar solicitações HTTP a partir de um navegador web, você precisa usar plug-ins de navegador para API REST. Você também pode acessar a API REST usando plataformas de script como cURL e Perl.

Autenticação

O Unified Manager suporta o esquema básico de autenticação HTTP para APIs. Para garantir um fluxo seguro de informações (solicitação e resposta), as APIs REST são acessíveis somente via HTTPS. O servidor da API fornece um certificado SSL autoassinado a todos os clientes para verificação do servidor. Esse certificado pode ser substituído por um certificado personalizado (ou certificado de CA).

Você deve configurar o acesso do usuário ao servidor da 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 da API para autenticar via LDAP). Você pode gerenciar o acesso do usuário fazendo login na interface de usuário do console de administração do Unified Manager.

Saiba mais sobre os códigos de status HTTP do 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 após a execução bem-sucedida de chamadas de API síncronas.
201	Criado	Criação de novos recursos por meio de chamadas síncronas, como a configuração do Active Directory.
202	Aceito	Retornado após a execução bem-sucedida de chamadas assíncronas para funções de provisionamento, como a criação de LUNs e compartilhamentos de arquivos.
400	Solicitação inválida	Indica falha na validação de entrada. Você precisa corrigir as entradas, por exemplo, chaves válidas no corpo da requisição.
401	Solicitação não autorizada	Você não está autorizado a visualizar o recurso/Não autorizado.
403	Solicitação proibida	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 dentro de um período específico.

Código de status HTTP	Título do código de status	Descrição
500	Erro interno do servidor	Erro interno do servidor. Falha ao obter a resposta do servidor. Esse erro interno do servidor pode ou não ser permanente. Por exemplo, se você executar uma `GET` ou `GET ALL` operação e receber esse erro, é recomendável repetir essa operação no mínimo cinco vezes. Se for um erro permanente, o código de status retornado continuará a ser 500. Se a operação for bem-sucedida, o código de status retornado será 200.

Siga as práticas recomendadas para usar o Active IQ Unified Manager APIs

Ao utilizar as APIs no Active IQ Unified Manager, você deve seguir algumas práticas recomendadas.

- Todo tipo de conteúdo da 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 a sua instância do Unified Manager. Para obter mais informações sobre as versões da API do Unified Manager, consulte a seção “Controle de versão da API REST no Active IQ Unified Manager”.
- Ao atualizar valores de um array usando a API do Unified Manager, você deve atualizar toda a sequência de valores. Não é possível adicionar valores a um array. Você só pode substituir um array existente.
- Você pode usar operadores de filtro, como pipe (|) e curinga (*), para todos os parâmetros de consulta, exceto para valores double, por exemplo, IOPS e desempenho, nas APIs de métricas.
- Evite consultar objetos usando uma combinação dos operadores de filtro curinga (*) e pipe (|). Isso pode retornar um número incorreto de objetos.
- Ao usar valores para filtro, certifique-se de que o valor não contenha nenhum `?` caractere. Isso serve para mitigar os riscos de injeção de SQL.
- Observe que a `GET`solicitação (total) para qualquer API retorna um máximo de 1000 registros. Mesmo que você execute a consulta definindo o `max_records`parâmetro para um valor superior a 1000, a API retorna apenas 1000 registros.
- Para executar funções administrativas, é recomendável que você use a interface de usuário do Unified Manager.

Solucione problemas com registros do sistema no Active IQ Unified Manager

Os registros do sistema permitem analisar as causas de falhas e problemas de troubleshooting que possam surgir durante a execução das APIs.

Recupere os logs do seguinte local para solucionar problemas relacionados às chamadas da API.

Localização do log	Usar
`/var/log/ocie/access_log.log`	Contém todos os detalhes da chamada da API, como o nome de usuário que invocou a API, horário de início, tempo de execução, status e URL. Você pode usar este arquivo de log para verificar as APIs mais usadas ou solucionar problemas em qualquer fluxo de trabalho da interface gráfica. Você também pode usá-lo para escalar a análise com base no tempo de execução.
`/var/log/ocum/ocumserver.log`	Contém todos os registros de execução da API. Você pode usar este arquivo de log para solucionar problemas e depurar as chamadas da API.
`/var/log/ocie/server.log`	Contém todos os registros de implantação do servidor Wildfly e os logs relacionados ao início/parada do serviço. 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.
`/var/log/ocie/au.log`	Contém registros relacionados à unidade de aquisição. Você pode usar este arquivo de log quando tiver criado, modificado ou excluído objetos no ONTAP, mas eles não forem refletidos nas APIs REST do Active IQ Unified Manager.

Entenda como o Active IQ Unified Manager utiliza objetos Job para processamento assíncrono

O Active IQ Unified Manager fornece a `jobs` API que recupera informações sobre os Jobs executados durante a execução de outras APIs. Você deve saber como o processamento assíncrono funciona usando o objeto Job.

Algumas chamadas de API, principalmente aquelas usadas para adicionar ou modificar recursos, podem demorar mais para serem concluídas do que outras. O Unified Manager processa essas solicitações de longa duração de forma assíncrona.

Solicitações assíncronas descritas usando o objeto Job

Após uma chamada de API assíncrona, o código de resposta HTTP 202 indica que a solicitação foi validada e aceita com sucesso, mas ainda não foi concluída. A solicitação é processada como uma tarefa em segundo plano que continua a ser executada após a resposta HTTP inicial ao cliente. A resposta inclui o objeto Job 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`

Existem duas técnicas que você pode usar ao consultar um objeto Job para detectar o estado final da tarefa, seja sucesso ou falha:

- Solicitação de sondagem padrão: o estado atual do trabalho é retornado imediatamente.
- Solicitação de long polling: quando o estado do trabalho passa 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 até que o objeto Job atinja o estado terminal `NORMAL, ERROR,` ou `PARTIAL_FAILURES.`
5. Verifique o estado terminal do Job e recupere o resultado do Job.

Saiba mais sobre o programa de exemplo do servidor Hello API no Active IQ Unified Manager

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 o formato `application/json`).

O URI utilizado é: `https://<hostname>/api/datacenter/svm/svms`. Este código de exemplo recebe os seguintes parâmetros de entrada:

- O endereço IP ou FQDN do servidor da API
- Opcional: número da porta (padrão: 443)
- Nome de usuário
- Senha
- Formato da resposta (`application/json`)

Para invocar APIs REST, você também pode usar outros scripts, como Jersey e RESTEasy, para escrever um

cliente REST Java para o Active IQ Unified Manager. Você deve estar ciente das seguintes considerações sobre o código de exemplo:

- Utiliza 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
- Usa `javax.net.ssl.HttpsURLConnection` para uma conexão de URI
- Utiliza uma biblioteca de terceiro (`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 HttpsURLConnection
getAllTrustingHttpsUrlConnection()    {        HttpsURLConnection conn =
null;        try {            /* Creating a trust manager that does not
validate certificate chains */            TrustManager[]
trustAllCertificatesManager = new                    TrustManager[]{new
X509TrustManager(){
     public X509Certificate[] getAcceptedIssuers(){return  null;}
     public void checkClientTrusted(X509Certificate[]
certs, String authType){}
     public void checkServerTrusted(X509Certificate[]
certs, String authType){}            }};            /* Initialize the
SSLContext with the all-trusting trust manager */
     SSLContext sslContext = SSLContext.getInstance("TLS");
sslContext.init(null, trustAllCertificatesManager, new
```

```
SecureRandom());
HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));            URL url = new URL(server_url);            conn =
(HttpsURLConnection) url.openConnection();            /* Do not perform an
actual hostname verification during SSL Handshake.            Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {               public
boolean verify(String host, SSLSession                        session) {
return true;               }            });        } catch (Exception e)
{            e.printStackTrace();        }        return conn;    }

    /*
     * * This forms the Base64 encoded string using the username and
password *
     * provided by the user. This is required for HTTP Basic
Authentication.
     */ private static String getAuthorizationString() {
        String userPassword = user + ":" + password;
        byte[] authEncodedBytes =
Base64.encodeBase64(userPassword.getBytes());
        String authString = new String(authEncodedBytes);
        return authString;
    }

}
```

APIs REST do Unified Manager

Entenda as categorias para as APIs REST do Active IQ Unified Manager

As APIs REST do Active IQ Unified Manager estão listadas nesta seção, com base em suas categorias.

Você pode visualizar a página da documentação online na 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 localizá-la na página da documentação. Após localizar uma chamada de API específica, você pode revisar os detalhes completos dessa chamada, incluindo os parâmetros de entrada, os formatos de saída, os códigos de status HTTP e o tipo de processamento da solicitação.

As informações a seguir 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 da API estão 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 correspondente.

- Verbo HTTP (chamada)

  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 utiliza 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.

Gerencie objetos de armazenamento em um data center usando APIs no Active IQ Unified Manager

As APIs REST na `datacenter` categoria permitem gerenciar 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 realizar operações como adicionar, excluir ou modificar esses objetos.

A maioria dessas APIs é composta por 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 no próximo ciclo de aquisição para aparecer na resposta.

Se você deseja consultar os detalhes de um objeto específico, precisa inserir o ID exclusivo desse objeto para visualizar seus detalhes. Por exemplo, para obter as métricas e as informações de análise dos objetos de storage, 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 da API Swagger. Você pode filtrar e ordenar os resultados por parâmetros específicos, conforme indicado no Swagger. Essas APIs permitem filtrar os resultados para objetos de storage específicos, como cluster, volume ou máquina virtual de storage.

APIs para objetos de storage em seu data center

Verbo HTTP	Caminho	Descrição
GET	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}	Você pode usar este método para visualizar os detalhes dos clusters do ONTAP em todo o data center. A API retorna informações, como o endereço IPv4 ou IPv6 do cluster, informações sobre o nó, como a integridade do nó, a capacidade de desempenho e o par de alta disponibilidade (HA), e indica se o cluster é um All SAN Array.
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 os resultados com base nos critérios desejados. São retornadas informações como a chave da licença, a chave do cluster, a data de expiração e o escopo da licença. Você pode inserir uma chave da 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. É possível 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, também são retornadas informações sobre a Lista de Controle de Acesso (ACL).

Verbo HTTP	Caminho	Descrição
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 dos serviços NFS compatíveis. Você pode consultar as políticas de exportação de um cluster ou de uma máquina virtual 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 “Provisioning CIFS and NFS file shares”.
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	Você pode usar esse método para visualizar o conjunto de agregados no data center ou um agregado específico para provisionar cargas de trabalho neles ou para monitoramento. São retornadas informações, como detalhes do cluster e do nó, capacidade de desempenho usada, espaço disponível e usado e eficiência de storage.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	Você pode usar esse método para visualizar o conjunto 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. São retornadas informações, como os detalhes do cluster e da SVM, os detalhes da política fixa ou adaptável e o número de objetos aplicáveis a essa política.

Verbo HTTP	Caminho	Descrição
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	Você pode usar este método para visualizar os detalhes do qtree em todo o data center para todos os volumes FlexVol ou volumes FlexGroup. São retornadas informações, como os detalhes do cluster e da SVM, o volume FlexVol e a política de exportação.
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	Você pode usar este método para visualizar a coleção de volumes no data center. São retornadas informações sobre os volumes, como detalhes de SVM e cluster, políticas de QoS e exportação, e se o volume é do tipo leitura/gravação, proteção de dados ou balanceamento de carga. Para os 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.

Verbo HTTP	Caminho	Descrição

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/protocols/san/igroups`
	
	`/datacenter/protocols/san/igroups/{key}`
		Você pode atribuir grupos de iniciadores (igroups) autorizados a acessar destinos LUN específicos. Se já existir um igroup, você pode 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 observar:
		
		• `POST`: Ao criar um igroup, você pode designar a VM de armazenamento à qual deseja atribuir acesso.
		• `DELETE`: Você precisa fornecer a chave do 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 do igroup como parâmetro de entrada para modificar um igroup específico. Você também deve inserir a propriedade que deseja atualizar, juntamente com o seu valor.

Verbo HTTP	Caminho	Descrição

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/svm/svms`
	
	`/datacenter/svm/svms/{key}`
		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 máquina virtual de armazenamento que deseja criar como parâmetro de entrada. Você pode criar uma máquina virtual 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 máquina virtual de armazenamento para modificar uma máquina virtual de armazenamento específica. Você também precisa inserir as propriedades que deseja atualizar, juntamente com seus valores.

Pontos a observar:

Se você habilitou o provisionamento de cargas de trabalho baseado em SLO (Objetivo de Nível de Serviço) no 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 nela, 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. Também é recomendável habilitar na VM de armazenamento os serviços para os respectivos tipos de cargas de trabalho.

Se você habilitou o provisionamento de cargas de trabalho baseado em SLO (Objetivo de Nível de Serviço) no seu ambiente, não poderá excluir a VM de armazenamento na qual as cargas de trabalho de armazenamento foram provisionadas. Ao excluir 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 Active Directory.

APIs para elementos de rede em seu data center

As APIs a seguir, na categoria de data center, recuperam informações sobre as portas e interfaces de rede em seu ambiente, especificamente as portas FC, interfaces FC, portas ethernet e interfaces IP.

Verbo HTTP	Caminho	Descrição
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	Recupera informações sobre todas as portas Ethernet no ambiente do seu data center. Com uma chave de porta como parâmetro de entrada, você pode visualizar as informações dessa porta específica. Recupera informações como detalhes do cluster, domínio de broadcast, detalhes da porta, como estado, velocidade e tipo, e se a porta está habilitada.
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. São obtidas informações como detalhes do cluster, detalhes do nó inicial e detalhes da porta inicial.
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. Recupera informações como detalhes do cluster, descrição da porta, protocolo suportado e o estado da porta.
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. São recuperadas informações como detalhes do cluster, detalhes do IPspace, detalhes do nó inicial e se o failover está habilitado.

Acesse as APIs do ONTAP por meio de acesso proxy no Active IQ Unified Manager

As APIs do gateway oferecem a você 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 está habilitado na interface da web do Unified Manager.

As APIs REST do Unified Manager suportam apenas um conjunto seleto de ações a serem executadas nas fontes de dados do Unified Manager, ou seja, clusters do ONTAP. Você pode usar os outros recursos por meio das APIs do ONTAP. As APIs de gateway permitem que o Unified Manager funcione como uma interface de passagem para encapsular em túnel todas as solicitações de API a serem executadas nos clusters do ONTAP que ele gerencia, sem a necessidade de fazer login em cada cluster do data center individualmente. Ele atua como um ponto único de gerenciamento para executar as APIs nos clusters do ONTAP gerenciados pela sua instância do Unified Manager. O recurso API Gateway permite que o Unified Manager seja um plano de controle único a partir do qual você pode gerenciar vários clusters do ONTAP, sem precisar fazer login em cada um deles individualmente. As APIs de gateway permitem que você permaneça conectado ao Unified Manager e gerencie os clusters do 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 da API REST do ONTAP.

O gateway atua como um proxy para encapsular as solicitações da API, mantendo o cabeçalho e o corpo das solicitações no mesmo formato das APIs do ONTAP. Você pode usar suas credenciais do Unified Manager e executar operações específicas para acessar e gerenciar os clusters do ONTAP sem precisar informar credenciais individuais de cada cluster. Ele continua gerenciando a autenticação e o gerenciamento do cluster, mas redireciona as solicitações da 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 oferecem suporte a chamadas de API REST do ONTAP. Você pode verificar os detalhes do cluster e optar por executar outros métodos com base no UUID do cluster, ou identificador único universal (UUID). As APIs do gateway recuperam apenas os clusters compatíveis com ONTAP 9.5 ou posterior e adicionados ao Unified Manager via 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 de API REST deve ser realizada. Além disso, certifique-se de que o UUID seja do cluster compatível com o ONTAP 9.5 ou posterior e adicionado ao Unified Manager por HTTPS. {path} deve ser substituído pela URL REST do ONTAP. Você deve remover `/api/` da URL.
		Esta é uma API proxy de ponto único, com suporte a operações POST, DELETE, PATCH e GET para todas as APIs REST do ONTAP. Não há restrições para nenhuma das APIs, desde que sejam suportadas pelo ONTAP. A funcionalidade de tunelamento ou proxy não pode ser desativada.
		
		O `OPTIONS` método retorna todas as operações suportadas por uma API REST do ONTAP. Por exemplo, se uma API do ONTAP oferecer suporte apenas à `GET` operação, executar o `OPTIONS` método usando esta API de gateway retornará `GET` como resposta. Este método não é compatível com o Swagger, mas pode ser executado em outras ferramentas de API.
		
		O `OPTIONS` método determina se um recurso está disponível. Essa operação pode ser usada para visualizar os metadados sobre um recurso nos cabeçalhos de resposta HTTP. Este método não é compatível com o Swagger, mas pode ser executado em outras ferramentas de API.

Entenda o tunelamento do API Gateway

As APIs do gateway permitem que você gerencie objetos do ONTAP por meio do Unified Manager. O Unified Manager gerencia os clusters e os detalhes de autenticação e redireciona as solicitações para o endpoint da API REST do ONTAP. A API do gateway transforma a URL e os links HATEOAS (Hypermedia as the Engine of Application State) no cabeçalho e no 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 da API REST do ONTAP e executa o endpoint da API REST do ONTAP necessário.

Para que uma API do ONTAP seja executada com sucesso por meio do gateway de API, a API deve ser compatível com essa versão do cluster do ONTAP em que está sendo executada. Executar uma API que não é compatível com o cluster do ONTAP não retornará nenhum resultado.

Neste exemplo, a API do gateway (URL base do proxy) é: `/gateways/{uuid}/`

A API do ONTAP usada é: `/storage/volumes`. Você precisa adicionar a URL da API REST do ONTAP como valor do parâmetro path.

Ao adicionar o caminho, certifique-se de ter removido o “/” symbol at the beginning of the URL. For the API `/storage/volumes`, add `storage/volumes`.

A URL anexada é: `/gateways/{uuid}/storage/volumes`

Ao executar a `GET` operação, a URL gerada é a seguinte:
`GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes`

A tag `/api` da URL da API REST do ONTAP é removida na URL anexada, e a da API de 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 storage nesse cluster. O formato da resposta é o mesmo que você recebe ao executar a mesma API no ONTAP. Os códigos de status retornados são os códigos de status REST do ONTAP.

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 storage também têm o cluster como escopo, ou seja, as operações da API são executadas em uma VM de storage específica dentro de um cluster gerenciado. Ao executar a `/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 storage específica dentro desse cluster, insira a chave da VM de storage como o parâmetro X-Dot-SVM-UUID ou o nome da VM de storage 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 storage nesse 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 como usar as APIs REST do ONTAP, consulte "Automação da API REST do ONTAP"

Execute tarefas administrativas usando APIs no Active IQ Unified Manager

Você pode usar as APIs na categoria `administration` para modificar as configurações de backup, verificar as informações do arquivo de backup e os certificados do cluster, além de gerenciar clusters ONTAP como fontes de dados do Active IQ Unified Manager.

Você precisa ter a função de Administrador de Aplicativos para executar essas operações. Você

também pode usar a interface web do Unified Manager para configurar 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 configurado no Unified Manager por padrão. Você pode verificar o seguinte:
		• Se o agendamento está ativado ou desativado
		• Frequência do backup agendado (diário 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 dump de backup é gerado sempre que a programação de backup é modificada para o Unified Manager. Você pode usar esse método para verificar se o arquivo de backup é gerado de acordo com as configurações de backup modificadas e se as informações no arquivo correspondem às configurações modificadas.
`GET`	`/admin/datasource-certificate`	Você pode usar este método para visualizar o certificado da fonte de dados (cluster) no repositório de confiança. A validação do certificado é necessária antes de adicionar um cluster ONTAP como uma fonte de dados do Unified Manager.

Verbo HTTP	Caminho	Descrição

`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 do ONTAP) gerenciadas pelo Unified Manager.
		
		Você também pode adicionar um novo cluster ao Unified Manager como uma fonte de dados. Para adicionar um cluster, você precisa saber o nome do host, o nome de usuário e a senha.
		
		Para modificar e excluir um cluster gerenciado como fonte de dados pelo Unified Manager, use a chave do cluster ONTAP.

Gerencie usuários no Active IQ Unified Manager usando APIs

Você pode usar as APIs desta `security`categoria para controlar o acesso de usuários a objetos de cluster selecionados no Active IQ Unified Manager. Você pode adicionar usuários locais ou usuários do banco de dados. Você também pode adicionar usuários remotos ou grupos que pertencem a um servidor de autenticação. Com base nos privilégios das funções que você atribui aos usuários, eles podem gerenciar os objetos de storage ou visualizar os dados no Unified Manager.

Você precisa ter a função de Administrador de Aplicativos para executar essas operações. Você também pode usar a interface web do Unified Manager para configurar essas configurações.

As APIs na categoria `security` utilizam o parâmetro users, ou seja, o nome de usuário, e não o parâmetro key como identificador único da entidade de usuário.

Verbo HTTP	Caminho	Descrição

`GET`
 	
`POST`
	`/security/users`
	
	`/security/users`
		Você pode usar esses métodos para obter detalhes dos usuários ou adicionar um novo usuário ao Unified Manager.
		
		Você pode adicionar funções específicas aos usuários com base em seus tipos de usuário. Ao adicionar usuários, você deve fornecer senhas para o usuário local, o usuário de manutenção e o usuário do banco de dados.

Verbo HTTP	Caminho	Descrição

`GET`
 	
`PATCH`
 	
`DELETE`
	`/security/users/{name}`	O método GET permite recuperar todos os detalhes de um usuário, como nome, endereço de e-mail, função e tipo de autorização. O método PATCH permite atualizar esses detalhes. O método DELETE permite remover o usuário.

Visualize métricas de desempenho usando APIs no Active IQ Unified Manager

O Active IQ Unified Manager fornece a você um conjunto de APIs na categoria `/datacenter` que permite visualizar os dados de desempenho de 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.

As `/metrics` e `/analytics` APIs oferecem diferentes visualizações das métricas de desempenho, com as quais você pode detalhar diferentes níveis de detalhe para os seguintes objetos de armazenamento em seu data center:

- clusters
- nós
- VMs de armazenamento
- agregados
- volumes
- LUNs
- Interfaces FC
- Portas FC
- Portas Ethernet
- Interfaces IP

A tabela a seguir faz uma comparação entre as `/metrics` e `/analytics` APIs com relação às especificidades dos dados de desempenho obtidos.

Métricas	Análises
Detalhes de desempenho para um único objeto. Por exemplo, a `/datacenter/cluster/clusters/{key}/metrics` API exige que a chave do cluster seja inserida como parâmetro de caminho para recuperar as métricas desse cluster específico.	Detalhes de desempenho para múltiplos objetos do mesmo tipo em um data center. Por exemplo, a `/datacenter/cluster/clusters/analytics` API recupera as métricas coletivas de todos os clusters em um data center.

Métricas	Análises
Amostra de métricas de desempenho para um objeto de armazenamento com base no parâmetro de intervalo de tempo para recuperação.	O valor agregado de alto nível do desempenho de um determinado tipo de objeto de armazenamento durante um determinado período (acima de 72 horas).
Os detalhes básicos do objeto são recuperados, como informações sobre um nó ou cluster.	Não se recupera nenhum detalhe específico.
O sistema recupera, para um único objeto, contadores acumulados, como mínimo, máximo, 95º percentil e valores médios de desempenho ao longo de um período, como contadores de leitura, gravação, total e outros.	Um único valor agregado é exibido para todos os objetos do mesmo tipo.

Métricas	Análises
O intervalo de tempo e os dados de amostra se baseiam na seguinte programação: o intervalo de tempo para os dados. Os exemplos podem ser 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m. Você obtém amostras de 1 hora se o intervalo for superior a 3 dias (72 horas); caso contrário, as amostras serão de 5 minutos. O período para cada intervalo de tempo é o seguinte: • 1h: métricas da última hora, amostradas em intervalos de 5 minutos. • 12h: métricas das últimas 12 horas, com amostragem em intervalos de 5 minutos. • 1d: métricas do dia mais recente, amostradas em intervalos de 5 minutos. • 2d: métricas dos últimos 2 dias, amostradas em intervalos de 5 minutos. • 3d: métricas dos últimos 3 dias, amostradas em intervalos de 5 minutos. • 15d: métricas dos últimos 15 dias, amostradas em intervalos de 1 hora. • 1w: 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 em 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, a `/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 durante o período apresentam um valor de contador inferior ao 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, a `/datacenter/cluster/nodes/analytics` API recupera os seguintes valores (entre outros) para todos os nós:

```
{     "iops": 1.7471,
     "latency": 60.0933,
     "throughput": 5548.4678,
     "utilization_percent": 4.8569,
     "period": 72,
     "performance_capacity": {
       "used_percent": 5.475,
       "available_iops_percent": 168350
     },
     "node": {
       "key": "37387241-8b57-11e9-8974-
00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a",
       "uuid": "95f94e8d-8b4e-11e9-8974-00a098e0219a",
       "name": "ocum-infinity-01",
       "_links": {
         "self": {
           "href": "/api/datacenter/cluster/nodes/37387241-8b57-11e9-8974-
00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a"
         }
       }
     },
     "cluster": {
```

```
        "key": "37387241-8b57-11e9-8974-
00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a",
        "uuid": "37387241-8b57-11e9-8974-00a098e0219a",
        "name": "ocum-infinity",
        "_links": {
          "self": {
            "href": "/api/datacenter/cluster/clusters/37387241-8b57-11e9-
8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a"
          },
      "_links": {
        "self": {
          "href": "/api/datacenter/cluster/nodes/analytics"
        }
      }
    },
```

Lista das APIs disponíveis

A tabela a seguir descreve em detalhes as APIs `/metrics` e `/analytics`.

> As métricas de IOPS e de desempenho retornadas por essas APIs são valores double, por exemplo `100.53`. Não há suporte para filtrar esses valores float 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. Retorna informações como a chave e o UUID do cluster, o intervalo de tempo, IOPS, a taxa de transferência e o número de amostras.
`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. Retorna valores como IOPS agregados, throughput e o período de coleta (em horas).

Verbo HTTP	Caminho	Descrição
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. Retorna informações como o UUID do nó, o intervalo de tempo, o resumo de IOPS, a taxa de transferência, a latência e o desempenho, o número de amostras coletadas e a porcentagem utilizada.
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. São retornadas informações, como chaves de nó e cluster, e valores, como IOPS agregados, throughput e o período de coleta (em horas).
GET	/datacenter/storage/aggregates/{key}/metrics	Recupera dados de desempenho (amostra e resumo) para um agregado especificado pelo parâmetro de entrada da chave do agregado. Retorna informações como o intervalo de tempo, o resumo de IOPS, a latência, a taxa de transferência e a capacidade de desempenho, o número de amostras coletadas para cada contador e a porcentagem utilizada.
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. Retorna informações, como chaves de agregados e clusters, e valores, como IOPS agregados, throughput e o período de coleta (em horas).

Verbo HTTP	Caminho	Descrição

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 arquivos (volume) especificado pelo parâmetro de entrada da chave do LUN ou do volume. São retornadas informações, como o resumo dos valores mínimo, máximo e médio de IOPS de leitura, gravação e total, latência e taxa de transferência, além do número de amostras coletadas para cada contador.

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 VM de armazenamento e de cluster, e valores, como IOPS agregados, throughput e o período de coleta (em horas), são retornadas.

GET	`/datacenter/svm/svms/{key}/metrics`	Recupera dados de desempenho (amostra e resumo) para uma máquina virtual de armazenamento especificada pelo parâmetro de entrada da chave da máquina virtual de armazenamento. São retornados o resumo de IOPS com base em cada protocolo compatível, como `nvmf, fcp, iscsi,` e `nfs`, a taxa de transferência, a latência e o número de amostras coletadas.
GET	`/datacenter/svm/svms/analytics`	Recupera métricas de alto nível para todas as VMs de armazenamento em um data center. Você pode filtrar seus resultados com base nos critérios necessários. São retornadas informações, como UUID da VM de armazenamento, IOPS agregadas, latência, throughput e o período de coleta (em horas).

Verbo HTTP	Caminho	Descrição
GET	/datacenter/network/ethernet/ports/{key}/metrics	Recupera as métricas de desempenho de uma porta Ethernet específica, especificada pelo parâmetro de entrada da chave da porta. Quando um intervalo (intervalo de tempo) é fornecido dentro do intervalo suportado, a API retorna os contadores acumulados, como os valores mínimo, máximo e médio de desempenho durante o período.
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. São retornadas informações, como a chave e o UUID do cluster e do nó, a taxa de transferência, o período de coleta e a porcentagem de utilização das portas. Você pode filtrar o resultado pelos parâmetros disponíveis, como a chave da porta, a porcentagem de utilização, o nome e o UUID do cluster e do nó, entre outros.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Recupera as métricas de desempenho de uma interface FC de rede específica, especificada pelo parâmetro de entrada da chave da interface. Quando um intervalo (período de tempo) é fornecido dentro do intervalo suportado, a API retorna os contadores acumulados, como os valores mínimo, máximo e médio de desempenho durante o período.

Verbo HTTP	Caminho	Descrição
GET	/datacenter/network/fc/interfaces/analytics	Recupera as métricas de desempenho de alto nível de todas as portas Ethernet em seu ambiente de data center. São retornadas informações, como o cluster e a chave e o UUID da interface FC, a taxa de transferência, IOPS, latência e a máquina virtual de armazenamento. Você pode filtrar o resultado pelos parâmetros disponíveis, como o nome e o UUID do cluster e da interface FC, a máquina virtual de armazenamento, a taxa de transferência e assim por diante.
GET	/datacenter/network/fc/ports/{key}/metrics	Recupera as métricas de desempenho de uma porta FC específica, especificada pelo parâmetro de entrada da chave da porta. Quando um intervalo (período de tempo) é fornecido dentro do intervalo suportado, a API retorna os contadores acumulados, como os valores mínimo, máximo e médio de desempenho durante o período.
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. São retornadas informações como a chave e o UUID do cluster e do nó, a taxa de transferência, o período de coleta e a porcentagem de utilização das portas. Você pode filtrar o resultado pelos parâmetros disponíveis, como a chave da porta, a porcentagem de utilização, o nome e o UUID do cluster e do nó, entre outros.

Verbo HTTP	Caminho	Descrição
GET	/datacenter/network/ip/interfaces/{key}/metrics	Recupera as métricas de desempenho de uma interface IP de rede, conforme especificado pelo parâmetro de entrada da chave da interface. Quando um intervalo (faixa de tempo) é fornecido dentro da faixa suportada, a API retorna informações como o número de amostras, contadores acumulados, taxa de transferência e o número de pacotes recebidos e transmitidos.
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. São retornadas informações como a chave e o UUID do cluster e da interface IP, a taxa de transferência, IOPS e a latência. Você pode filtrar o resultado pelos parâmetros disponíveis, como o nome e o UUID do cluster e da interface IP, IOPS, latência, taxa de transferência e assim por diante.

Visualize tarefas e detalhes do sistema usando APIs no Active IQ Unified Manager

Você pode usar a `jobs`API na categoria `management-server` para visualizar os detalhes de execução de operações assíncronas. A `system`API na categoria `management-server` permite que você visualize os detalhes da instância em seu ambiente do Active IQ Unified Manager.

Ver trabalhos

No Active IQ Unified Manager, operações, como adicionar e modificar recursos, são realizadas por meio de invocações de API síncronas e assíncronas. As invocações agendadas para execução assíncrona podem ser rastreadas por um objeto Job criado para essa invocação. Cada objeto Job possui uma chave exclusiva para identificação. Cada objeto Job retorna o URI do objeto Job para que você possa acessar e acompanhar o progresso da tarefa. Você pode usar essa API para recuperar os detalhes de cada execução.

Ao usar esta API, você pode consultar todos os os objetos Job do seu data center, incluindo dados históricos. Por padrão, a consulta de todos os jobs retorna os detalhes dos últimos 20 jobs acionados pela interface web e pela interface de API. Use os filtros integrados para visualizar Jobs específicos. Você também pode usar a chave do Job para consultar os detalhes de um job específico e executar o próximo conjunto de operações nos recursos.

Categoria	Verbo HTTP	Caminho	Descrição
servidor de gerenciamento	GET	`/management-server/jobs`	Retorna os detalhes de todos os jobs. Sem nenhuma ordem de classificação, o último objeto Job enviado aparece no topo.
servidor de gerenciamento	GET	`/management-server/jobs/{key}` Insira a chave do objeto Job para visualizar os detalhes específicos desse job.	Retorna os detalhes do objeto Job específico.

Ver detalhes do sistema

Ao usar a `/management-server/system` API, você pode consultar os detalhes específicos da instância do seu ambiente do Unified Manager. A API retorna informações sobre o produto e os serviços, como a versão do Unified Manager instalada no 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	GET	`/management-server/system`	Não é necessário nenhum parâmetro de entrada para executar esta API. Os detalhes do sistema da instância atual do Unified Manager são retornados por padrão.

Gerencie eventos e alertas usando APIs no Active IQ Unified Manager

As APIs `events`, `alerts` e `scripts` na categoria `management-server` permitem que você gerencie os eventos, alertas e os scripts associados aos alertas no seu ambiente do Active IQ Unified Manager.

Visualizar e modificar eventos

O Unified Manager recebe os eventos gerados no ONTAP para os clusters monitorados e gerenciados pelo Unified Manager. Usando essas APIs, você pode visualizar os eventos gerados para seus clusters, além de resolvê-los e atualizá-los.

Ao executar o `GET`método da `/management-server/events`API, você pode consultar os eventos em seu data center, incluindo dados históricos. Use os filtros integrados, 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 informações sobre o problema que gerou o evento, 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 obter mais informações sobre eventos, consulte "Saiba mais sobre os eventos da plataforma Active IQ".

Categoria	Verbo HTTP	Caminho	Descrição
servidor de gerenciamento	GET	`/management-server/events` `/management-server/events/{key}`	Ao executar o método Get ALL, o corpo da resposta consiste nos detalhes de todos os eventos em 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	PATCH	`management-server/events/{key}`	Execute esta API para atribuir um evento ou alterar o estado para reconhecido ou resolvido. Você também pode usar este método para atribuir o evento a si mesmo ou a outro usuário. É uma operação síncrona.

Gerenciar alertas

Os eventos são gerados de forma automática e contínua. 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 a `/management-server/alerts` API, você pode configurar alertas para enviar notificações automaticamente quando ocorrerem eventos específicos ou eventos de determinados níveis de gravidade.

Para obter mais informações sobre alertas, consulte "Saiba mais sobre alertas".

Categoria	Verbo HTTP	Caminho	Descrição
servidor de gerenciamento	GET	`/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 informações sobre os alertas gerados no seu ambiente, como a descrição do alerta, a ação, o endereço de e-mail para o qual a notificação é enviada, o evento e a gravidade.
servidor de gerenciamento	POST	`/management-server/alerts`	Este método permite adicionar alertas para eventos específicos. Você deve adicionar o nome do alerta, o recurso físico ou lógico, ou o evento ao qual o alerta se aplica, 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 endereço de 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, além de 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 apenas para eventos críticos do cluster. Você não receberá alertas para eventos críticos em nós, agregados e assim por diante.

Gerenciar scripts

Ao usar a `/management-server/scripts` API, você também pode associar um alerta a um script que é executado quando um alerta é acionado. Você pode usar scripts para modificar ou atualizar automaticamente vários objetos de armazenamento no Unified Manager. O script fica associado a um alerta. Quando um evento aciona um alerta, o script é executado. Você pode fazer upload de scripts personalizados e testar sua execução quando um alerta é gerado. Você pode associar um alerta ao seu script para que o script seja executado quando um alerta for gerado para um evento no Unified Manager.

Para obter mais informações sobre scripts, consulte "Gerenciar scripts".

Categoria	Verbo HTTP	Caminho	Descrição
servidor de gerenciamento	GET	`/management-server/scripts`	Use esta API para consultar todos os scripts existentes no seu ambiente. Use os filtros padrão e as operações de ordenação para visualizar apenas scripts específicos.
servidor de gerenciamento	POST	`/management-server/scripts`	Use esta API para adicionar uma descrição ao script e fazer upload do arquivo de script associado a um alerta.

Gerencie cargas de trabalho

Visualize as cargas de trabalho de armazenamento usando APIs no Active IQ Unified Manager

As APIs listadas aqui permitem que você visualize uma lista consolidada de cargas de trabalho de storage de todos os clusters do ONTAP em seu data center. As APIs também fornecem uma visão resumida do número de cargas de trabalho de storage provisionadas em seu ambiente do Active IQ Unified Manager, bem como suas estatísticas de capacidade e desempenho (IOPS).

Visualizar cargas de trabalho de storage

Você pode usar o seguinte método para visualizar todas as cargas de trabalho de storage 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	GET	`/storage-provider/workloads`

Visualizar resumo das cargas de trabalho de storage

Você pode usar o seguinte método para avaliar a capacidade utilizada, a capacidade disponível, os IOPS utilizados, os IOPS disponíveis e o número de cargas de trabalho de storage gerenciadas por cada Nível de Serviço de Desempenho. As cargas de trabalho de storage exibidas podem ser de qualquer LUN,

compartilhamento de arquivos NFS ou compartilhamento CIFS. A API fornece uma visão geral das cargas de trabalho de storage, uma visão geral das cargas de trabalho de storage provisionadas pelo Unified Manager, uma visão geral do data center e uma visão geral do espaço total, utilizado e disponível e dos 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 IU do Unified Manager.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/storage-provider/workloads-summary`

Gerencie endpoints de acesso usando APIs no Active IQ Unified Manager

Você precisa criar endpoints de acesso ou interfaces lógicas (LIFs), que são necessários para provisionar as Storage Virtual Machines (SVMs), os LUNs e os compartilhamentos de arquivos. Você pode visualizar, criar, modificar e excluir os endpoints de acesso para as SVMs, os LUNs ou os compartilhamentos de arquivos em seu ambiente do Active IQ Unified Manager.

Visualizar endpoints de acesso

Você pode visualizar uma lista dos pontos de extremidade de acesso em seu ambiente do Unified Manager usando o seguinte método. Para consultar uma lista de pontos de extremidade de acesso de uma SVM, LUN ou compartilhamento de arquivos específico, você precisa inserir o identificador exclusivo da SVM, LUN ou do 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	GET	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

Adicionar pontos de extremidade de acesso

Você pode criar endpoints de acesso personalizados e atribuir as propriedades necessárias a eles. Você deve inserir os detalhes do endpoint de acesso que deseja criar como parâmetros de entrada. Você pode usar esta API, o System Manager ou a CLI do ONTAP para criar um endpoint de acesso em cada nó. Há suporte para endereços IPv4 e IPv6 na criação de endpoints de acesso.

> Você deve configurar sua SVM com um número mínimo de endpoints de acesso por nó para o provisionamento bem-sucedido de LUNs e compartilhamentos de arquivos. Você deve configurar sua SVM com pelo menos dois endpoints de acesso por nó, um com suporte ao protocolo CIFS e/ou NFS e outro com suporte ao protocolo iSCSI ou FCP.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	POST	`/storage-provider/access-endpoints`

Excluir pontos de extremidade de acesso

Você pode excluir um endpoint de acesso específico usando o seguinte método. Você precisa fornecer a chave do endpoint de acesso como parâmetro de entrada para excluir um endpoint de acesso específico.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	EXCLUIR	`/storage-provider/access-endpoints/{key}`

Modificar endpoints de acesso

Você pode modificar um endpoint de acesso e atualizar suas propriedades usando o seguinte método. Você precisa fornecer a chave do endpoint de acesso para modificar um endpoint de acesso específico. Você também precisa inserir a propriedade que deseja atualizar, juntamente com seu valor.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	PATCH	`/storage-provider/access-endpoints/{key}`

Gerencie mapeamentos do Active Directory usando APIs no Active IQ Unified Manager

Você pode usar as APIs listadas aqui para gerenciar os mapeamentos do Active Directory na SVM necessários para o provisionamento de compartilhamentos CIFS nas SVMs. Os mapeamentos do Active Directory precisam ser configurados para mapear as SVMs com 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 da SVM. Para consultar os detalhes de um mapeamento específico, você deve inserir a chave do mapeamento.

Categoria	Verbo HTTP	Caminho

provedor de armazenamento	GET	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

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	POST	`/storage-provider/active-directories-mappings`

Gerencie compartilhamentos de arquivos usando APIs no Active IQ Unified Manager

Você pode usar a `/storage-provider/file-shares` API para visualizar, adicionar, modificar e excluir os volumes de compartilhamento de arquivos CIFS e NFS em seu ambiente de data center.

Antes de provisionar os volumes de compartilhamento de arquivos, certifique-se de que a SVM tenha sido criada e provisionada 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 devem ser criados antes de criar os compartilhamentos de arquivos.

Visualizar 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 fonte de dados no Active IQ Unified Manager, as cargas de trabalho de storage desses clusters são adicionadas automaticamente à sua instância do Unified Manager. Esta API recupera os compartilhamentos de arquivos adicionados automática e manualmente à sua instância do Unified Manager. Você pode visualizar os detalhes de um compartilhamento de arquivos específico executando esta API com a chave do compartilhamento de arquivos.

Categoria	Verbo HTTP	Caminho

provedor de armazenamento	GET	`/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 na sua SVM. Você deve inserir os detalhes do compartilhamento de arquivos que deseja criar como parâmetros de entrada. Não é possível usar esta API para adicionar volumes FlexGroup.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	POST	`/storage-provider/file-shares`

Dependendo de serem fornecidos os parâmetros da lista de controle de acesso (ACL) ou os parâmetros da política de exportação, serão criados compartilhamentos CIFS ou compartilhamentos de arquivos NFS. Se você não fornecer os valores dos parâmetros da ACL, os compartilhamentos CIFS não serão criados, e os compartilhamentos NFS serão criados por padrão, fornecendo acesso a todos.

Criação de volumes de proteção de dados: ao adicionar compartilhamentos de arquivos à sua SVM, o tipo do volume montado, por padrão, é `rw` (leitura e gravação). Para criar volumes de proteção de dados (DP), especifique `dp` como valor para o `type` parâmetro.

Excluir compartilhamentos de arquivos

Você pode usar o seguinte método para excluir um compartilhamento de arquivos específico. Você precisa inserir a chave do compartilhamento de arquivos como parâmetro de entrada para excluir um

compartilhamento de arquivos 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.

Para modificar um compartilhamento de arquivos específico, você precisa fornecer a chave do compartilhamento de arquivos. Além disso, você precisa inserir a propriedade que deseja atualizar, juntamente com seu valor.

Observe que você só pode atualizar uma propriedade por vez ao invocar esta API. Para várias atualizações, você precisa executar esta API várias vezes.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	PATCH	`/storage-provider/file-shares/{key}`

Gerencie LUNs usando APIs no Active IQ Unified Manager

Você pode usar a `/storage-provider/luns` API para visualizar, adicionar, modificar e excluir as LUNs no seu ambiente de data center.

Antes de provisionar os LUNs, certifique-se de que a SVM foi criada e provisionada 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 devem ser criados antes da criação do LUN.

Ver LUNs

Você pode usar o método a seguir para visualizar os LUNs no seu ambiente do Unified Manager. Quando você adiciona um cluster ONTAP como fonte de dados no Active IQ Unified Manager, as cargas de trabalho de storage desses clusters são adicionadas automaticamente à sua instância do Unified Manager. Esta API recupera todos os LUNs adicionados automática e manualmente à sua instância do Unified Manager. Você pode visualizar os detalhes de um LUN específico executando esta API com a chave do LUN.

Categoria	Verbo HTTP	Caminho

provedor de armazenamento	GET	`/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	POST	`/storage-provider/luns`

Na sua requisição 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. Essa tag facilita a busca pelo volume. Se você fornecer a chave do volume na requisição, a atribuição da tag será ignorada.

Excluir LUNs

Você pode usar o seguinte método para excluir um LUN específico. Você precisa fornecer a chave do LUN para excluir um LUN em particular.

Se você criou um volume no ONTAP e provisionou LUNs por meio do Unified Manager nesse volume, ao excluir todas as LUNs usando esta API, o volume também é excluído do cluster do 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. É necessário fornecer a chave do LUN para modificar um LUN específico. Você também precisa inserir a propriedade do LUN que deseja atualizar, juntamente com seu valor. Para atualizar arrays de LUN usando esta API, consulte as recomendações em “Recommendations for using the APIs”.

Você pode atualizar apenas uma propriedade por vez ao invocar esta API. Para várias atualizações, você precisa executar esta API várias vezes.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	PATCH	`/storage-provider/luns/{key}`

Gerencie os níveis de serviço de desempenho usando APIs no Active IQ Unified Manager

Você pode visualizar, criar, modificar e excluir níveis de serviço de desempenho usando as APIs do provedor de storage no seu Active IQ Unified Manager.

Visualizar níveis de serviço de desempenho

Você pode usar o seguinte método para visualizar os níveis de serviço de desempenho para atribuí-los às cargas de trabalho de storage. A API lista todos os níveis de serviço de desempenho definidos pelo sistema e criados pelo usuário, e recupera os atributos de todos os níveis de serviço de desempenho. Se você quiser consultar um nível de serviço de desempenho específico, precisará inserir o ID exclusivo do nível de serviço de desempenho para obter seus detalhes.

Categoria	Verbo HTTP	Caminho

provedor de armazenamento	GET	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

Adicionar Níveis de Serviço de Desempenho

Você pode usar o seguinte método para criar os Performance Service Levels personalizados e atribuí-los às suas cargas de trabalho de storage se os Performance Service Levels definidos pelo sistema não atenderem aos objetivos de nível de serviço (SLOs) necessários para as cargas de trabalho de storage. Insira os detalhes do Performance Service Level que você deseja criar. Para as propriedades de IOPS, certifique-se de inserir um intervalo válido de valores.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	POST	`/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. Para excluir um Nível de Serviço de Desempenho específico, você precisa fornecer o ID exclusivo do Nível de Serviço de Desempenho como parâmetro de entrada.

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. Para modificar um Nível de Serviço de Desempenho específico, você precisa fornecer o ID exclusivo. Além disso, você deve inserir a propriedade de IOPS que deseja atualizar, juntamente com um valor válido.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	PATCH	`/storage-provider/performance-service-levels/{key}`

Visualize as capacidades do agregado com base nos Níveis de Serviço de Desempenho

Você pode usar o seguinte método para consultar os recursos do agregado com base nos Performance Service Levels. Esta API retorna a lista de agregados disponíveis em seu data center e indica os recursos em termos dos Performance Service Levels que podem ser suportados nesses agregados. Ao provisionar cargas de trabalho em um volume, você pode ver a capacidade de um agregado de oferecer suporte a um Performance Service Level 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. Essa funcionalidade não está disponível na interface web do Unified Manager.

Categoria	Verbo HTTP	Caminho

provedor de armazenamento	GET	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

Gerencie políticas de eficiência de armazenamento usando APIs no Active IQ Unified Manager

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.
- Você não pode remover 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 do ONTAP, como deduplicação e compactação, essas configurações poderão ser substituídas pelas configurações especificadas na Storage Efficiency Policy que você aplica ao adicionar as cargas de trabalho de armazenamento no Unified Manager.

Ver as políticas de eficiência de armazenamento

Você pode usar o seguinte método 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 você quiser consultar uma Política de Eficiência de Armazenamento específica, precisará inserir o ID exclusivo da política para recuperar seus detalhes.

Categoria	Verbo HTTP	Caminho

provedor de armazenamento	GET	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

Adicionar políticas de eficiência de armazenamento

Você pode usar o seguinte método para criar políticas de eficiência de armazenamento personalizadas e atribuí-las às suas cargas de trabalho de armazenamento caso as políticas definidas pelo sistema não atendam aos requisitos de provisionamento das 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	POST	`/storage-provider/storage-efficiency-policies`

Excluir políticas de eficiência de armazenamento

Você pode usar o seguinte método para excluir uma Storage Efficiency Policy específica. Não é possível excluir uma Storage Efficiency Policy se ela estiver atribuída a uma carga de trabalho ou se for a única Storage Efficiency Policy disponível. Para excluir uma Storage Efficiency Policy específica, você precisa fornecer o ID exclusivo da Storage Efficiency Policy como parâmetro de entrada.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	EXCLUIR	`/storage-provider/storage-efficiency-policies/{key}`

Modificar as 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. Para modificar uma Política de Eficiência de Armazenamento específica, você precisa fornecer o ID exclusivo da Política de Eficiência de Armazenamento. Além disso, você precisa fornecer a propriedade que deseja atualizar, juntamente com seu valor.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	PATCH	`/storage-provider/storage-efficiency-policies/{key}`

Fluxos de trabalho comuns para gerenciamento de storage

Compreenda os fluxos de trabalho comuns da API para gerenciamento de storage no Active IQ Unified Manager

Os fluxos de trabalho comuns fornecem aos desenvolvedores de aplicativos cliente exemplos de como as APIs do Active IQ Unified Manager podem ser chamadas por um aplicativo cliente para executar funções comuns de gerenciamento de storage. Esta seção contém alguns desses fluxos de trabalho de exemplo.

Os fluxos de trabalho descrevem alguns dos casos de uso de gerenciamento de storage mais comuns, juntamente com exemplos de código para você usar. Cada tarefa é descrita por meio de um processo de fluxo de trabalho que consiste em uma ou mais chamadas de API.

Compreenda as chamadas de API utilizadas nos fluxos de trabalho

Você pode visualizar a página de documentação online da sua instância do Unified Manager, que inclui os detalhes de cada chamada de API REST. Este documento não repete os detalhes da documentação online. Cada chamada de API usada nos exemplos de fluxo de trabalho neste documento inclui apenas as informações de que você precisa 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, os formatos de saída, os códigos de status HTTP e o tipo de processamento da solicitação.

As informações a seguir 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 da API estão 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 correspondente.
- Verbo HTTP (chamada): 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.

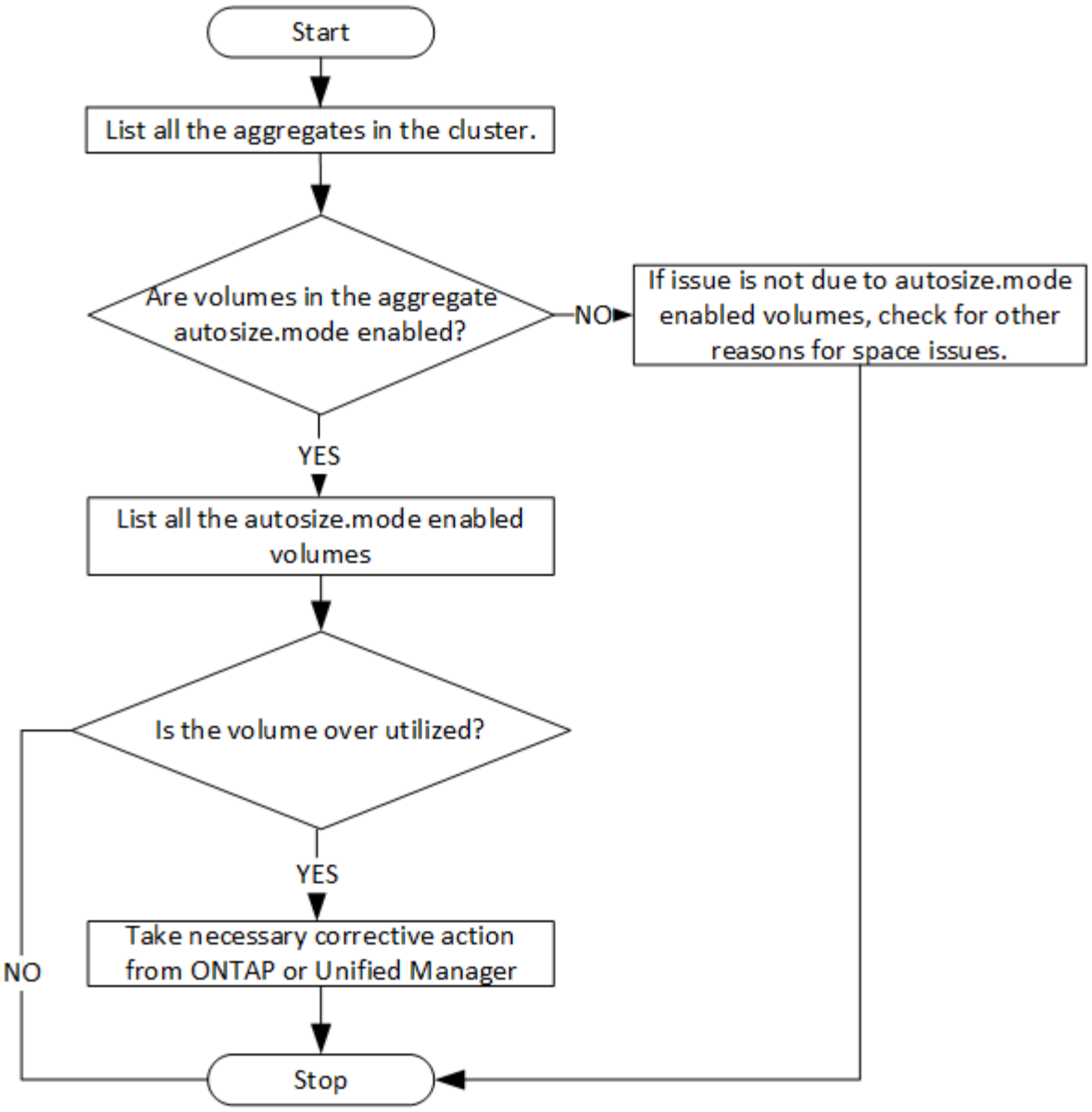
Identifique problemas de espaço em agregados usando as APIs do Active IQ Unified Manager

Você pode usar as APIs de 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 em seu volume e identificar recursos de storage que estão sobreutilizados ou subutilizados.

As APIs de data center para agregados recuperam as informações relevantes sobre o espaço disponível e utilizado, bem como as configurações de eficiência de economia de espaço. Você também pode filtrar as informações recuperadas com base em atributos específicos.

Uma maneira de determinar qualquer falta de espaço em seus agregados é verificar se existem volumes em seu ambiente com o modo de dimensionamento automático ativado. Em seguida, você deve identificar quais volumes estão sendo excessivamente utilizados e executar as ações corretivas necessárias.

O fluxograma a seguir ilustra o processo de recuperação de informações sobre volumes com o modo de dimensionamento automático ativado:



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 já saiba o valor:

Categoria	Verbo HTTP	Caminho
data center	GET	`/datacenter/cluster/clusters`

2. Utilizando a chave do cluster como parâmetro de filtro, consulte os agregados nesse cluster.

Categoria	Verbo HTTP	Caminho
data center	GET	`/datacenter/storage/aggregates`

3. A partir da resposta, analise o uso de espaço dos agregados e determine quais agregados apresentam problemas de espaço. Para cada agregado com problema de espaço, obtenha a chave do agregado na mesma saída JSON.

4. Usando cada chave de agregado, filtre todos os volumes que têm o valor do parâmetro autosize.mode como `grow`.

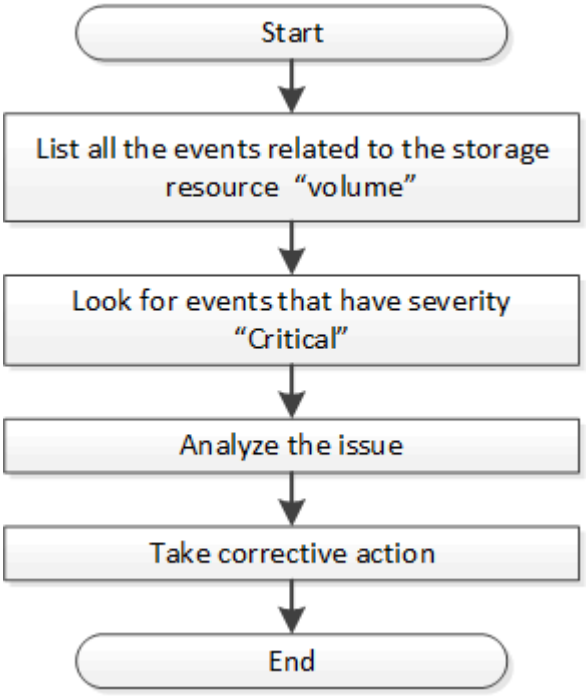
Categoria	Verbo HTTP	Caminho
data center	GET	`/datacenter/storage/volumes`

5. Analise quais volumes estão sendo utilizados em excesso.
6. Execute as ações corretivas necessárias, como mover o volume entre agregados, para resolver os problemas de espaço no seu volume. Você pode executar essas ações na interface web do ONTAP ou do Unified Manager.

Identifique problemas com objetos de armazenamento usando o Active IQ Unified Manager event APIs

Quando um objeto de armazenamento em seu data center ultrapassa um limite, você recebe uma notificação sobre esse evento. Usando essa notificação, você pode analisar o problema e tomar medidas corretivas por meio das `events` APIs.

Este fluxo de trabalho usa o exemplo de um volume como objeto de recurso. Você pode usar as `events` APIs para recuperar a lista de eventos relacionados a um volume, analisar os problemas críticos desse volume e, em seguida, tomar medidas corretivas para solucionar o problema.



Siga estes passos para identificar 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	GET	/management-server/events

3. Visualize a saída e analise os problemas nos volumes específicos.
4. Execute as ações necessárias usando as APIs REST do Unified Manager ou a interface da web para resolver os problemas.

Solucione problemas dos volumes ONTAP usando as APIs de gateway do Active IQ Unified Manager

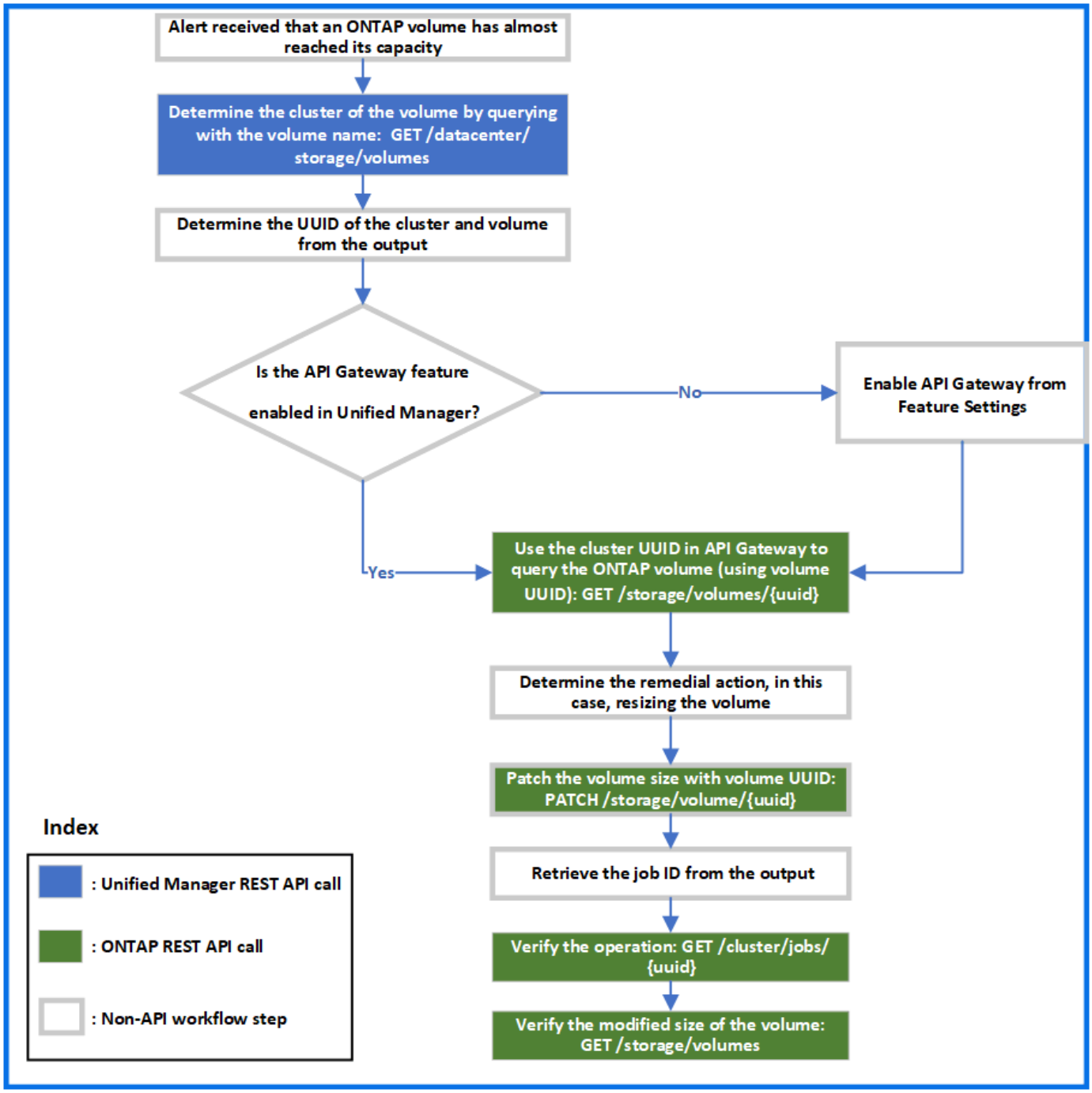
As APIs de gateway atuam como uma porta de entrada para invocar as APIs do ONTAP, consultar informações sobre seus objetos de armazenamento do ONTAP e tomar medidas corretivas para solucionar os problemas relatados.

Este fluxo de trabalho aborda um exemplo de caso de uso em que um evento é acionado quando um volume do ONTAP quase atinge sua capacidade. O fluxo de trabalho também demonstra como resolver esse problema invocando uma combinação das APIs REST do Active IQ Unified Manager e do ONTAP.

Antes de executar as etapas do fluxo de trabalho, certifique-se do seguinte:

- Você está ciente das APIs do gateway e de como elas são usadas. Para obter informações, consulte "Acesso às APIs do ONTAP por meio de acesso por proxy".
- Você conhece o uso das APIs REST do ONTAP. Para obter informações sobre como usar as APIs REST do ONTAP, consulte "Documentação de automação do 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 você adiciona o cluster ao Unified Manager via HTTPS.

O diagrama a seguir ilustra cada etapa do fluxo de trabalho para solucionar o problema de uso da capacidade do volume do ONTAP.



O fluxo de trabalho abrange os pontos de invocação das APIs REST do Unified Manager e do ONTAP.

1. Anote o nome do volume no evento que notifica a utilização da capacidade do volume.
2. Utilizando o nome do volume como valor no parâmetro `name`, consulte o volume executando a seguinte API do Unified Manager.

Categoria	Verbo HTTP	Caminho
data center	GET	`/datacenter/storage/volumes`

3. Recupere o UUID do cluster e o UUID do volume da saída.

4. Na interface do usuário da web do Unified Manager, navegue até **General** > **Feature Settings** > **API Gateway** para verificar se o recurso API Gateway está habilitado. A menos que ele esteja habilitado, as APIs na categoria gateway não estarão disponíveis para você invocar. Habilite o recurso se ele estiver desabilitado.
5. Utilize o UUID do cluster para executar a API ONTAP `/storage/volumes/{uuid}` por meio 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 pelo gateway de API, as credenciais do Unified Manager são passadas internamente para autenticação, e você não precisa executar uma etapa adicional de autenticação para acesso a clusters individuais.

Categoria	Verbo HTTP	Caminho
O Unified Manager: gateway ONTAP: armazenamento	GET	A API Gateway: `/gateways/{uuid}/{path}` API ONTAP: `/storage/volumes/{uuid}`

   Em /gateways/{uuid}/{path}, o valor de {uuid} deve ser substituído pelo UUID do cluster no qual a operação da API REST deve ser realizada. {path} deve ser substituído pelo URL REST do ONTAP /storage/volumes/{uuid}.

   A URL anexada 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>"
```

6. A partir da saída, determine o tamanho, o uso e a medida corretiva a ser tomada. Neste fluxo de trabalho, a medida corretiva tomada é o redimensionamento do volume.
7. Use o UUID do cluster e execute a seguinte API do 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
O Unified Manager: gateway ONTAP: armazenamento	PATCH	A API Gateway: `/gateways/{uuid}/{path}` API ONTAP: `/storage/volumes/{uuid}`

Juntamente com o UUID do cluster e o UUID do volume, você deve inserir um valor para o parâmetro size 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 tarefa.

8. Verifique se a tarefa foi executada com sucesso usando o UUID da tarefa. Use o UUID do cluster e o UUID da tarefa para executar a seguinte API do ONTAP por meio do gateway de API. Para obter informações sobre os parâmetros de entrada das APIs do gateway e do ONTAP, consulte a etapa 5.

Categoria	Verbo HTTP	Caminho
O Unified Manager: gateway O ONTAP: cluster	GET	A API Gateway: `/gateways/{uuid}/{path}` API do ONTAP: `/cluster/jobs/{uuid}`

Os códigos HTTP retornados são os mesmos códigos de status HTTP da API REST do ONTAP.

9. Execute a seguinte API ONTAP para consultar os detalhes do volume redimensionado. Para obter informações sobre os parâmetros de entrada para as APIs de gateway e ONTAP, consulte a etapa 5.

Categoria	Verbo HTTP	Caminho
O Unified Manager: gateway ONTAP: armazenamento	GET	A API Gateway: `/gateways/{uuid}/{path}` API ONTAP: `/storage/volumes/{uuid}`

A saída exibe um tamanho de volume aumentado de 120 GB.

Fluxos de trabalho para gerenciamento de carga de trabalho

Provisione e modifique cargas de trabalho de armazenamento no Active IQ Unified Manager

Usando o Active IQ Unified Manager, você pode provisionar e modificar cargas de trabalho de storage (LUNs, compartilhamentos de arquivos NFS e compartilhamentos CIFS). O provisionamento consiste em várias etapas, desde a criação da Storage Virtual Machine (SVM) até a aplicação de políticas de Performance Service Level e Storage

Efficiency nas cargas de trabalho de storage. A modificação de cargas de trabalho consiste nas etapas para modificar parâmetros específicos e habilitar recursos adicionais nelas.

Os fluxos de trabalho descritos a seguir são:

- Fluxo de trabalho para provisionamento de Máquinas Virtuais de Storage (SVMs) no Unified Manager.

  você precisa executar este fluxo de trabalho antes de provisionar LUNs ou compartilhamentos de arquivos no Unified Manager.

- Provisionamento de compartilhamentos de arquivos.
- Provisionamento de LUNs.
- Modificando LUNs e compartilhamentos de arquivos (usando o exemplo de atualização do parâmetro nível de serviço de desempenho para workloads de storage).
- Modificando um compartilhamento de arquivos NFS para oferecer suporte ao protocolo CIFS
- Modificando cargas de trabalho para atualizar o QoS para AQoS

Para cada fluxo de trabalho de provisionamento (LUN e compartilhamentos de arquivos), certifique-se de que concluiu 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 as SVMs em clusters ONTAP usando as APIs do Active IQ Unified Manager

Antes de provisionar compartilhamentos de arquivos ou LUNs, você deve verificar se os clusters têm Storage Virtual Machines (SVMs) criadas.

O fluxo de trabalho pressupõe que os clusters ONTAP tenham sido adicionados ao Unified Manager e que a chave do cluster tenha sido obtida. Os clusters devem ter as licenças necessárias para provisionar LUNs e compartilhamentos de arquivos neles.

1. Verifique se o cluster possui uma SVM criada.

Categoria	Verbo HTTP	Caminho
data center	GET	`/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>"
```

2. Se a chave da SVM não for retornada, crie a SVM. Para criar as SVMs, você precisa da chave do cluster

no qual provisiona a SVM. Você também precisa especificar o nome da SVM. Siga estas etapas.

Categoria	Verbo HTTP	Caminho
data center	GET	`/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>"
```

3. A partir da saída, obtenha a chave do cluster e, em seguida, use-a como entrada para criar a SVM.

> Ao criar a SVM, certifique-se de que ela suporte todos os protocolos necessários para o provisionamento de LUNs e compartilhamentos de arquivos nela, como CIFS, NFS, FCP e iSCSI. Os fluxos de trabalho de provisionamento podem falhar se a SVM não suportar os serviços necessários. Também é recomendável habilitar na SVM os serviços para os respectivos tipos de cargas de trabalho.

Categoria	Verbo HTTP	Caminho
data center	POST	`/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\" ] },
```

```
\"fcp\": { \"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 do objeto Job que você pode usar para verificar a SVM que você criou.

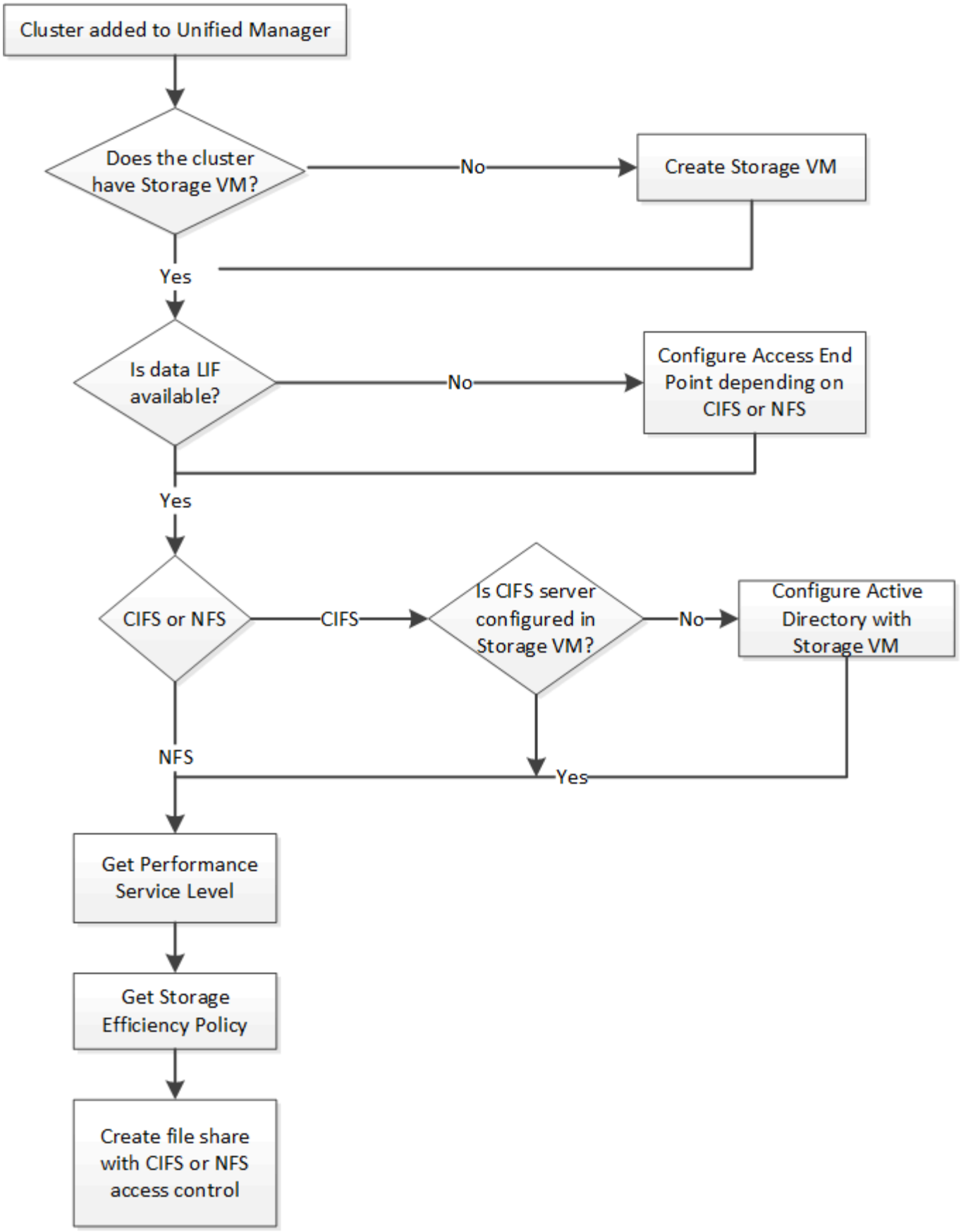
4. Verifique a criação da SVM usando a chave do objeto de job para a consulta. Se a SVM for criada com sucesso, a resposta retornará a chave da SVM.

Categoria	Verbo HTTP	Caminho
servidor de gerenciamento	GET	`/management-server/jobs/{key}`

Provisione compartilhamentos de arquivos CIFS e NFS usando as APIs do Active IQ Unified Manager

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 das SVMs, os Níveis de Serviço de Desempenho e as 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. Ele inclui o provisionamento de compartilhamentos CIFS e compartilhamentos de arquivos NFS.



Certifique-se do seguinte:

- Os clusters ONTAP foram adicionados ao Unified Manager, e a chave do cluster foi obtida.
- As SVMs foram criadas nos clusters.
- Os SVMs suportam os serviços CIFS e NFS. O provisionamento de compartilhamentos de arquivos pode falhar se os SVMs não suportarem os serviços necessários.
- A porta FCP está online para provisionamento de porta.

1. Verifique se as LIFs de dados ou os endpoints de acesso estão disponíveis na SVM na qual você deseja criar o compartilhamento CIFS. Obtenha a lista de endpoints de acesso disponíveis na SVM:

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/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 endpoint de acesso estiver disponível na lista, obtenha a chave do endpoint de acesso, caso contrário, crie o endpoint de acesso.

Certifique-se de criar endpoints de acesso com o protocolo CIFS habilitado. O provisionamento de compartilhamentos CIFS falhará, a menos que você tenha criado um endpoint de acesso com o protocolo CIFS habilitado.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	POST	`/storage-provider/access-endpoints`

Exemplo de cURL

Você deve inserir, como parâmetros de entrada, os detalhes do endpoint de acesso que deseja criar.

```
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 do objeto Job que você pode usar para verificar o endpoint de acesso que você criou.

3. Verifique o endpoint de acesso:

Categoria	Verbo HTTP	Caminho
servidor de gerenciamento	GET	`/management-server/jobs/{key}`

4. Determine se você precisa criar um compartilhamento CIFS ou um compartilhamento de arquivos NFS. Para criar compartilhamentos CIFS, siga estas subetapas:

   a. Verifique se o servidor CIFS está configurado na sua SVM, ou seja, verifique se há um mapeamento do Active Directory criado na SVM.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/storage-provider/active-directories-mappings`

   b. Se o mapeamento do Active Directory estiver criado, use a chave; caso contrário, crie o mapeamento do Active Directory na SVM.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	POST	`/storage-provider/active-directories-mappings`

Exemplo de cURL

Você deve inserir os detalhes para criar o mapeamento do Active Directory nos parâmetros de entrada.

```
curl -X POST "https://<hostname>/api/storage-provider/active-
directories-mappings" -H "accept: application/json" -H "Content-Type:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \"_links\": {},
\"dns\": \"10.000.000.000\",
\"domain\": \"example.com\",
```

```
\"password\": \"string\",
\"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-
005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },
\"username\": \"string\"}"
```

+
Esta é uma chamada síncrona e você pode verificar a criação do mapeamento do Active Directory na saída. Em caso de erro, a mensagem de erro é exibida para que você possa solucionar o problema e executar a solicitação novamente.

5. Obtenha a chave da SVM na qual você deseja criar o compartilhamento CIFS ou o compartilhamento de arquivos NFS, conforme descrito no tópico do fluxo de trabalho *Verifying SVMs on clusters*.
6. Obtenha a chave do nível de serviço de desempenho executando a seguinte API e recuperando a chave da resposta.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/storage-provider/performance-service-levels`

> Você pode recuperar os detalhes dos Níveis de Serviço de Desempenho definidos pelo sistema configurando o `system_defined` parâmetro de entrada como `true`. Na saída, obtenha a chave do Nível de Serviço de Desempenho que você deseja aplicar ao compartilhamento de arquivos.

7. Opcionalmente, obtenha a chave da Política de eficiência de storage que você deseja aplicar ao compartilhamento de arquivos executando a seguinte API e recuperando a chave da resposta.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/storage-provider/storage-efficiency-policies`

8. Crie o compartilhamento de arquivos. Você pode criar um compartilhamento de arquivos que suporte CIFS e NFS especificando a lista de controle de acesso e a política de exportação. As subetapas a seguir fornecem informações 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 após criar o compartilhamento NFS. Para obter informações, consulte o tópico *Modifying storage workloads*.

   a. Para criar apenas um compartilhamento CIFS, reúna as informações sobre a lista de controle de acesso (ACL). Para criar o compartilhamento CIFS, forneça valores válidos para os seguintes parâmetros de entrada. Para cada grupo de usuários que você atribuir, uma ACL é criada quando um compartilhamento CIFS/SMB é provisionado. Com base nos valores inseridos para ACL e mapeamento do Active Directory, o controle de acesso e o mapeamento são definidos para o compartilhamento CIFS quando ele é criado.

      Um comando cURL com valores de exemplo

```
{
  "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 nos 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 você quiser reutilizar uma política de exportação para a VM de storage, precisará adicionar a chave da política de exportação. A menos que você conheça a chave, pode recuperar a chave da política de exportação usando a `/datacenter/protocols/nfs/export-policies` API. Para criar uma nova política, você deve inserir as regras conforme mostrado no exemplo a seguir. Para as regras inseridas, a API tenta procurar uma política de exportação existente correspondendo ao host, à VM de storage 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 exemplo

```
"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 Storage Efficiency Policy é um parâmetro opcional para criar compartilhamentos de arquivos.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	POST	`/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 de objeto Job retornada na consulta ao job:

Categoria	Verbo HTTP	Caminho
servidor de gerenciamento	GET	`/management-server/jobs/{key}`

Ao final da resposta, você vê a chave do compartilhamento de arquivos 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	GET	`/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, ele invoca a `/storage-provider/performance-service-levels/` API para atribuir o Nível de Serviço de Desempenho ao 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": {}
```

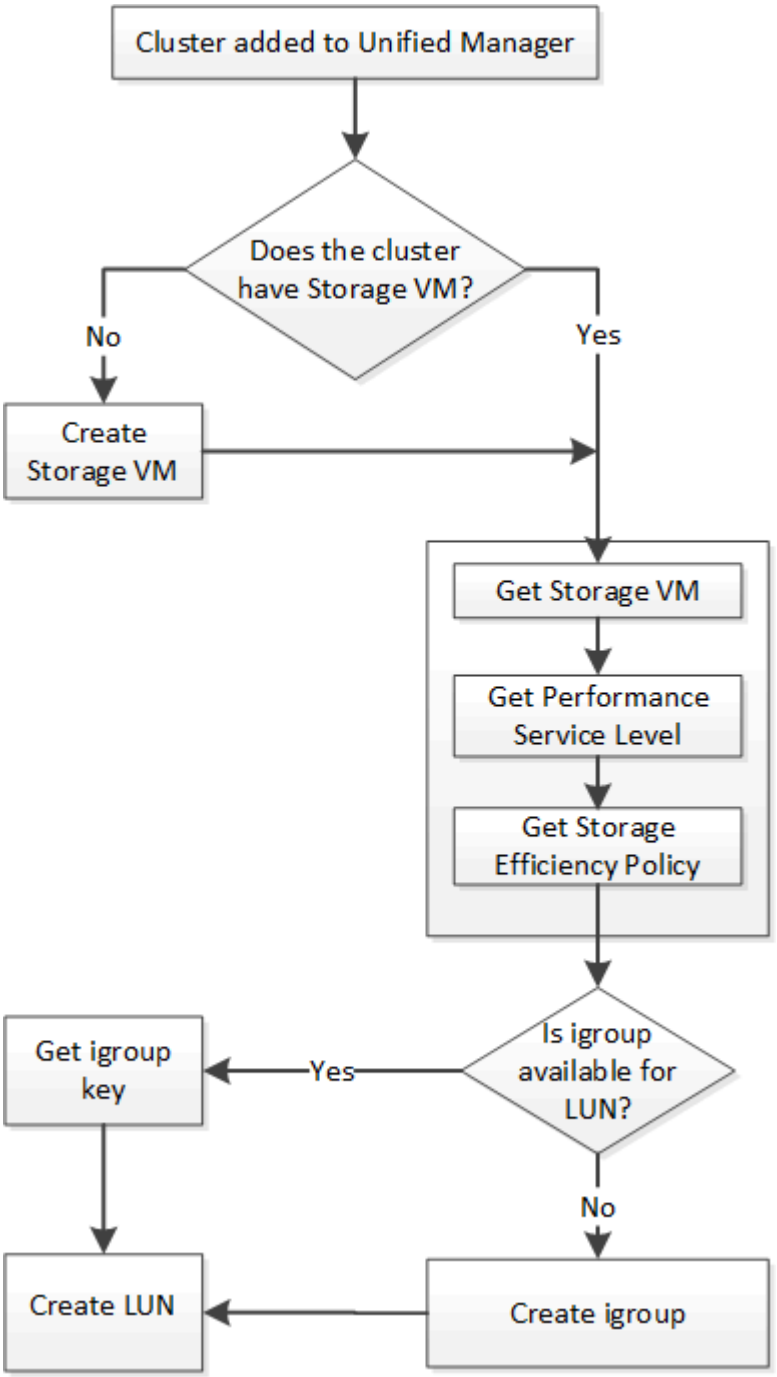
```
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "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 as APIs do Active IQ Unified Manager

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 das SVMs, os Níveis de Serviço de Desempenho e as Políticas de Eficiência de Armazenamento antes de criar a LUN.

O diagrama a seguir ilustra as etapas de 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 da SVM para a SVM na qual você deseja criar o LUN, conforme descrito no tópico de fluxo de trabalho *Verifying SVMs on clusters*.
2. Obtenha a chave do nível de serviço de desempenho executando a seguinte API e recuperando a chave da resposta.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/storage-provider/performance-service-levels`

Você pode obter os detalhes dos Níveis de Serviço de Desempenho definidos pelo sistema configurando o `system_defined` parâmetro de entrada para `true`. A partir da saída, obtenha a chave do Nível de Serviço de Desempenho que você deseja aplicar na LUN.

3. Opcionalmente, obtenha a chave da Política de Eficiência de Storage que você deseja aplicar à LUN executando a seguinte API e recuperando a chave da resposta.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/storage-provider/storage-efficiency-policies`

4. Verifique se grupos de iniciadores (igroups) foram criados para conceder acesso ao destino de LUN que você deseja criar.

Categoria	Verbo HTTP	Caminho
data center	GET	`/datacenter/protocols/san/igroups` `/datacenter/protocols/san/igroups/{key}`

Você deve inserir o valor do parâmetro para indicar a SVM para a qual o igroup tem acesso autorizado. Além disso, se desejar consultar um igroup específico, insira o nome (chave) do igroup como parâmetro de entrada.

5. Na saída, se você conseguir encontrar o igroup ao qual deseja conceder acesso, obtenha a chave. Caso contrário, crie o igroup.

Categoria	Verbo HTTP	Caminho
data center	POST	`/datacenter/protocols/san/igroups`

Você deve inserir os detalhes do igroup que deseja criar, como os parâmetros de entrada. Esta é uma chamada síncrona, e você pode verificar a criação do igroup na saída. Em caso de erro, uma mensagem é exibida para que você possa solucionar o problema e executar a API novamente.

6. Crie o LUN.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	POST	`/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 storage é um parâmetro opcional para criar LUNs.

Exemplo de cURL

Você deve inserir, como parâmetros de entrada, todos os detalhes da LUN que deseja criar.

A saída JSON exibe uma chave de objeto Job que você pode usar para verificar o LUN que você criou.

7. Verifique a criação da LUN usando a chave do objeto Job retornada na consulta ao Job:

Categoria	Verbo HTTP	Caminho
servidor de gerenciamento	GET	`/management-server/jobs/{key}`

Ao final da resposta, você verá a chave da LUN criada.

8. Verifique a criação da LUN executando a seguinte API com a chave retornada:

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/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, ele invoca a `/storage-provider/performance-service-levels/`API para atribuir o nível de serviço de desempenho ao LUN.

== Etapas de solução de problemas para falha na criação ou no mapeamento de LUN

Ao concluir este fluxo de trabalho, você ainda poderá encontrar 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 uma SAN LIF ou endpoint de acesso no nó em que você cria o LUN. Em caso de falha, você verá 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 estes passos de resolução de problemas para contornar essa falha.

1. Crie um endpoint de acesso que suporte o protocolo iSCSI/FCP na SVM na qual você tentou criar o LUN.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	POST	`/storage-provider/access-endpoints`

Exemplo de cURL

Você deve inserir os detalhes do endpoint 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 principal do LUN e o ha_address para indicar o nó parceiro do nó principal. Ao executar esta operação, são criados endpoints de acesso tanto no nó principal quanto no nó parceiro.

2. Consulte a tarefa com a chave do objeto Job retornada na saída JSON para verificar se ela foi executada com sucesso para adicionar os endpoints de acesso na SVM e se os serviços iSCSI/FCP foram habilitados na SVM.

Categoria	Verbo HTTP	Caminho
servidor de gerenciamento	GET	`/management-server/jobs/{key}`

Exemplo de saída JSON

Ao final da saída, você pode ver a chave dos endpoints de acesso criados. Na saída a seguir, o valor "name": "accessEndpointKey" indica o endpoint de acesso criado no nó home da LUN, cuja chave é 9c964258-14ef-11ea-95e2-00a098e32c28. O valor "name": "accessEndpointHAKey" indica o endpoint de acesso criado no nó parceiro do nó home, cuja chave é 9d347006-14ef-11ea-8760-00a098e3215f.

3. Modifique o LUN para atualizar o mapeamento do igroup. Para obter mais informações sobre a modificação do fluxo de trabalho, consulte “Modifying storage workloads”.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	PATCH	`/storage-provider/lun/{key}`

No campo de entrada, especifique a chave do igroup com a qual deseja atualizar o mapeamento de LUN, juntamente com a chave de 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 da LUN consultando a chave da LUN.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/storage-provider/luns/{key}`

Exemplo de saída JSON

Na saída, você pode ver que o LUN foi mapeado com sucesso para o igroup (chave d19ec2fa-fec7-11e8-b23d-00a098e32c28) com o qual foi provisionado inicialmente.

Modificar cargas de trabalho de storage

A modificação das cargas de trabalho de armazenamento consiste em atualizar LUNs ou compartilhamentos de arquivos com parâmetros ausentes ou em alterar os parâmetros existentes.

Este fluxo de trabalho usa como exemplo a atualização dos Níveis de Serviço de Desempenho para LUNs e compartilhamentos de arquivos.

O fluxo de trabalho pressupõe que o LUN ou compartilhamento de arquivos tenha sido provisionado com Níveis de Serviço de Desempenho.

Modificar compartilhamentos de arquivos

Ao modificar um compartilhamento de arquivos, 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).
- Configurações da política de exportação. Você também pode excluir parâmetros da política de exportação e restaurar as regras padrão (vazias) da política de exportação no compartilhamento de arquivos.

Durante uma única execução da 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 do compartilhamento de arquivos.

1. Obtenha a chave do compartilhamento CIFS ou do compartilhamento de arquivos NFS do compartilhamento de arquivos que você deseja atualizar. Esta API consulta todos os compartilhamentos de arquivos no seu data center. Ignore esta etapa se você já souber a chave do compartilhamento de arquivos.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/storage-provider/file-shares`

2. Veja os detalhes do compartilhamento de arquivos executando a seguinte API com a chave do compartilhamento de arquivos que você obteve.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/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 do Nível de Serviço de Desempenho que você deseja atribuir a este compartilhamento de arquivos. Atualmente nenhuma política está atribuída a ele.

Categoria	Verbo HTTP	Caminho
Níveis de serviço de desempenho	GET	`/storage-provider/performance-service-levels`

> Você pode obter os detalhes dos Níveis de Serviço de Desempenho definidos pelo sistema configurando o `system_defined` parâmetro de entrada para `true`. A partir da saída, obtenha a chave do Nível de Serviço de Desempenho que deseja aplicar ao compartilhamento de arquivos.

4. Aplique o Nível de Serviço de Desempenho ao compartilhamento de arquivos.

Categoria	Verbo HTTP	Caminho
Fornecedor de armazenamento	PATCH	`/storage-provider/file-shares/{key}`

Na entrada, você deve especificar apenas o parâmetro que deseja atualizar, juntamente com a chave de compartilhamento de arquivos. Neste caso, trata-se da 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 local 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	GET	`/management-server/jobs/{key}`

Ao consultar pelo ID do objeto Job, você pode verificar 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 visualizar o objeto modificado:

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	GET	`/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 uma LUN, você pode modificar os seguintes parâmetros:

- Capacidade ou tamanho
- Configuração online ou offline
- Política de Eficiência de Armazenamento
- Nível de serviço de desempenho
- Mapeamento de LUN

Durante uma única execução da API, você pode atualizar apenas um parâmetro.

Este procedimento descreve como adicionar um Nível de Serviço de Desempenho a uma LUN. Você pode usar o mesmo procedimento para atualizar qualquer outra propriedade da LUN.

1. Obtenha a chave LUN da LUN que você deseja atualizar. Esta API retorna detalhes de todas as LUNs em seu data center. Ignore esta etapa se você já souber a chave LUN.

Categoria	Verbo HTTP	Caminho
Fornecedor de armazenamento	GET	`/storage-provider/luns`

2. Para visualizar os detalhes da LUN, execute a seguinte API com a chave da LUN que você obteve.

Categoria	Verbo HTTP	Caminho
Fornecedor de armazenamento	GET	`/storage-provider/luns/{key}`

Veja os detalhes do LUN na saída. Você pode observar 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 do Performance Service Level que você deseja atribuir ao LUN.

Categoria	Verbo HTTP	Caminho
Níveis de serviço de desempenho	GET	`/storage-provider/performance-service-levels`

Você pode obter os detalhes dos Níveis de Serviço de Desempenho definidos pelo sistema configurando o `system_defined` parâmetro de entrada para `true`. A partir da saída, obtenha a chave do Nível de Serviço de Desempenho que você deseja aplicar na LUN.

4. Aplique o Nível de Serviço de Desempenho (PSL) no LUN.

Categoria	Verbo HTTP	Caminho
Fornecedor de armazenamento	PATCH	`/storage-provider/lun/{key}`

Na entrada, você deve especificar apenas o parâmetro que deseja atualizar, juntamente com a chave da LUN. Neste caso, trata-se da 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 do objeto Job que você pode usar para verificar o LUN que você atualizou.

5. Para visualizar os detalhes da LUN, execute a seguinte API com a chave da LUN que você obteve.

Categoria	Verbo HTTP	Caminho
Fornecedor de armazenamento	GET	`/storage-provider/luns/{key}`

Veja os detalhes do LUN na saída. Você pode ver que o Performance Service Level 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"
            }
```

Modifique um compartilhamento de arquivos NFS para suportar CIFS usando as APIs do Active IQ Unified Manager

Você pode modificar um compartilhamento de arquivos NFS para oferecer suporte ao protocolo CIFS. Durante a criação do compartilhamento de arquivos, é possível especificar os parâmetros da lista de controle de acesso (ACL) e as regras da política de exportação para o mesmo compartilhamento de arquivos. No entanto, se você quiser habilitar CIFS no mesmo volume em que criou um compartilhamento de arquivos NFS, poderá atualizar os parâmetros de ACL desse compartilhamento de arquivos para oferecer suporte a CIFS.

Antes de começar

1. É necessário criar um compartilhamento de arquivos NFS contendo apenas os detalhes da política de exportação. Para obter mais informações, consulte *Gerenciando compartilhamentos de arquivos* e *Modificando cargas de trabalho de armazenamento*.
2. Você precisa da chave do compartilhamento de arquivos para executar esta operação. Para obter informações sobre como visualizar os detalhes do compartilhamento de arquivos e recuperar a chave do

compartilhamento de arquivos usando o ID da tarefa, 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 de ACL.

Passos

1. No compartilhamento de arquivos NFS, execute uma `PATCH` operação com os detalhes da ACL para permitir o acesso CIFS.

Categoria	Verbo HTTP	Caminho
provedor de armazenamento	PATCH	`/storage-provider/file-shares`

Exemplo de cURL

Com base nos privilégios de acesso que você atribui ao grupo de usuários, conforme mostrado 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 Job ID do Job 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	GET	`/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 juntamente com a política de exportação para o mesmo compartilhamento de arquivos.

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e mais.

Direitos autorais

"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/"

Patentes

A lista atual de patentes detidas pela 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/"

Código aberto

Informações sobre direitos autorais e licenças de terceiros usados neste produto.

"Aviso para o Active IQ Unified Manager 9.18"

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.