Active IQ Unified Manager 文档

Active IQ Unified Manager

NetApp
November 13, 2026

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

目录

Active IQ Unified Manager 文档 1
Active IQ Unified Manager 发行说明 2
开始使用 3
在 VMware vSphere 上开始使用 Active IQ Unified Manager 3
系统要求 3
安装 Active IQ Unified Manager 3
在 Linux 上开始使用 Active IQ Unified Manager 4
系统要求 4
安装 Active IQ Unified Manager 4
在 Windows 上开始使用 Active IQ Unified Manager 5
系统要求 5
安装 Active IQ Unified Manager 5
在 VMware vSphere 系统上安装 Unified Manager 7
了解Active IQ Unified Manager 7
了解Active IQ Unified Manager 7
了解 Active IQ Unified Manager 服务器的作用 7
了解 Active IQ Unified Manager 安装顺序 7
安装 Unified Manager 的要求 8
确保服务器满足 Active IQ Unified Manager 安装要求 8
了解 Active IQ Unified Manager 的虚拟基础架构和硬件要求 8
了解 Active IQ Unified Manager 的 VMware 软件和安装要求 9
在 Active IQ Unified Manager 中使用受支持的浏览器 10
了解 Active IQ Unified Manager 的协议和端口要求 10
在 Active IQ Unified Manager 中填写工作表 13
在 VMware vSphere 上安装、升级和删除 Unified Manager 14
了解 Active IQ Unified Manager 部署流程 14
Unified Manager 虚拟设备部署工作流 15
Unified Manager 虚拟设备升级工作流 18
重新启动 Active IQ Unified Manager 虚拟机 21
删除 Active IQ Unified Manager 21
在 Linux 系统上安装 Unified Manager 23
Active IQ Unified Manager 简介 23
了解Active IQ Unified Manager 23
了解 Active IQ Unified Manager 服务器的作用 23
查看 Active IQ Unified Manager 的安装顺序 23
安装 Unified Manager 的要求 24
了解安装 Active IQ Unified Manager 的要求 24
了解 Active IQ Unified Manager 的虚拟基础架构和硬件要求 24
了解 Active IQ Unified Manager 中的 Linux 软件和安装要求 25

请使用支持的浏览器访问 Active IQ Unified Manager 27
了解 Active IQ Unified Manager 中的协议和端口要求 28
在 Active IQ Unified Manager 中填写工作表 30
安装、升级和删除 Unified Manager 软件 31
安装、升级和删除 Active IQ Unified Manager 软件 31
了解在 Red Hat Enterprise Linux 上安装 Active IQ Unified Manager 的顺序 31
设置所需的软件 32
在 Active IQ Unified Manager 中为 NFS 和 CIFS 共享配置 SELinux 35
在 Linux 系统上安装 Unified Manager 38
在 Red Hat Enterprise Linux 上升级 Unified Manager 43
安装 Unified Manager 后升级第三方产品 48
重新启动 Active IQ Unified Manager 49
删除 Active IQ Unified Manager 49
删除 Active IQ Unified Manager 的自定义 umadmin 用户和 maintenance 组 50
在 Windows 系统上安装 Unified Manager 51
Active IQ Unified Manager 简介 51
了解Active IQ Unified Manager 51
了解 Active IQ Unified Manager 服务器的作用 51
了解 Active IQ Unified Manager 的安装顺序 51
安装 Unified Manager 的要求 52
确保服务器满足 Active IQ Unified Manager 安装要求 52
了解 Active IQ Unified Manager 的虚拟基础架构和硬件要求 52
了解 Active IQ Unified Manager 的 Windows 软件和安装要求 53
在 Active IQ Unified Manager 中使用受支持的浏览器 55
了解 Active IQ Unified Manager 的协议和端口要求 55
在 Active IQ Unified Manager 中填写工作表 57
安装、升级和删除 Unified Manager 软件 58
了解在 Windows 上安装 Active IQ Unified Manager 的过程 58
在 Windows 上安装 Unified Manager 59
在 Active IQ Unified Manager 中更改 Windows 上的 JBoss 密码 62
请对 Active IQ Unified Manager 版本使用受支持的升级路径 63
在 Windows 上升级 Active IQ Unified Manager 63
升级第三方产品 65
卸载 Active IQ Unified Manager 中的第三方产品 65
在 Windows 上重新启动 Active IQ Unified Manager 66
卸载 Active IQ Unified Manager 67
执行配置和管理任务 68
配置 Active IQ Unified Manager 68
了解有关配置 Active IQ Unified Manager 的信息 68
了解 Active IQ Unified Manager 中的配置顺序 68
访问 Active IQ Unified Manager 中的 Web UI 68

执行 Active IQ Unified Manager Web UI 的初始设置 69
向 Active IQ Unified Manager 添加集群 71
配置通知 73
在 Active IQ Unified Manager 中更改本地用户密码 80
在 Active IQ Unified Manager 中设置会话非活动超时 81
使用 Active IQ Unified Manager 中的 CLI 设置会话超时 81
更改 Unified Manager 主机名 82
在 Active IQ Unified Manager 中启用和禁用基于策略的存储管理 85
配置 Active IQ Unified Manager 备份 86
管理功能设置 86
了解 Active IQ Unified Manager 中的功能设置 86
在 Active IQ Unified Manager 中启用基于策略的存储管理 86
了解 Active IQ Unified Manager 中的 API Gateway 功能 87
在 Active IQ Unified Manager 中指定非活动超时 87
在 Active IQ Unified Manager 中启用 Active IQ 门户事件 87
在 Active IQ Unified Manager 中启用和禁用合规性安全设置 88
在 Active IQ Unified Manager 中启用和禁用脚本上传 88
在 Active IQ Unified Manager 中添加登录横幅 89
使用维护控制台 89
了解 Active IQ Unified Manager 中的维护控制台 89
了解 Active IQ Unified Manager 中的维护用户 89
Active IQ Unified Manager 中的诊断用户功能 90
访问 Active IQ Unified Manager 中的维护控制台 90
使用 Active IQ Unified Manager 中的 vSphere VM 控制台访问维护控制台 90
维护控制台菜单 91
在 Windows 中更改 Active IQ Unified Manager 的维护用户密码 96
在 Linux 系统上更改 Active IQ Unified Manager umadmin 密码 96
更改 Active IQ Unified Manager 用于 HTTP 和 HTTPS 协议的端口 97
向 Active IQ Unified Manager 添加网络接口 97
在 Active IQ Unified Manager 中重新生成客户端证书 98
添加磁盘空间 98
管理用户访问 102
添加用户 102
在 Active IQ Unified Manager 中编辑用户设置 103
在 Active IQ Unified Manager 中查看用户 103
删除 Active IQ Unified Manager 中的用户或组 103
了解 Active IQ Unified Manager 中基于角色的访问控制 104
了解 Active IQ Unified Manager 中的用户类型 104
了解 Active IQ Unified Manager 中的用户角色 105
了解 Active IQ Unified Manager 中的用户角色和功能 106
管理 SAML 身份验证设置 107

在 Active IQ Unified Manager 中启用 SAML 身份验证 107
在 Active IQ Unified Manager 中使用身份提供程序 107
在 Active IQ Unified Manager 中启用 SAML 身份验证 108
在 Active IQ Unified Manager 中更改 SAML 身份验证标识提供程序 109
在 Active IQ Unified Manager 安全证书更改后更新 SAML 身份验证设置 109
在 Active IQ Unified Manager 中禁用 SAML 身份验证 110
从 Active IQ Unified Manager 维护控制台禁用 SAML 身份验证 111
使用 Active IQ Unified Manager 中的 SAML 身份验证页面 112
管理身份验证 112
在 Active IQ Unified Manager 中编辑身份验证服务器 113
删除 Active IQ Unified Manager 中的身份验证服务器 113
在 Active IQ Unified Manager 中使用 Active Directory 或 OpenLDAP 进行身份验证 113
审核日志记录 114
使用 Active IQ Unified Manager 中的远程身份验证页面 116
管理安全证书 119
在 Active IQ Unified Manager 中查看 HTTPS 安全证书 119
在 Active IQ Unified Manager 中下载 HTTPS 证书签名请求 119
在 Active IQ Unified Manager 中安装 CA 签名的 HTTPS 证书 119
了解在 Active IQ Unified Manager Unified Manager 中使用外部工具生成的 HTTPS 证书 120
证书管理的页面描述 123
监控和管理存储 125
Active IQ Unified Manager 简介 125
了解Active IQ Unified Manager 125
了解 Active IQ Unified Manager 中的运行状况监控 125
了解 Active IQ Unified Manager 中的性能监控 126
使用 Active IQ Unified Manager REST API 127
Unified Manager 服务器的功能 127
了解用户界面 128
了解 Active IQ Unified Manager 用户界面 128
Active IQ Unified Manager 中的典型窗口布局 128
在 Active IQ Unified Manager 中自定义窗口布局 129
使用 Active IQ Unified Manager 帮助 130
在 Active IQ Unified Manager 中收藏您喜爱的帮助主题 130
在 Active IQ Unified Manager 中搜索存储对象 130
将存储数据导出为 Active IQ Unified Manager 中的报告 132
在 Active IQ Unified Manager 中筛选清单页面内容 133
通过 Active IQ Unified Manager 中的通知铃查看活动事件 134
从仪表板监控和管理集群 134
通过 Active IQ Unified Manager 中的信息板监控和管理集群 134
了解 Active IQ Unified Manager 仪表板页面 135
直接从 Unified Manager 修复或管理 ONTAP 问题 137

管理集群 142
了解 Active IQ Unified Manager 中的集群发现过程如何工作 142
查看 Active IQ Unified Manager 监控的集群列表 143
向 Active IQ Unified Manager 添加集群 143
在 Active IQ Unified Manager 中编辑集群设置 146
从 Active IQ Unified Manager 中删除集群 146
在 Active IQ Unified Manager 中重新发现集群 147
监控 VMware 虚拟基础架构 147
了解 Active IQ Unified Manager 如何监控 VMware 虚拟基础架构 147
在 Active IQ Unified Manager 中查看和添加 vCenter Servers 151
从 Active IQ Unified Manager 中删除 vCenter Server 152
了解 Active IQ Unified Manager 如何监控虚拟机 153
使用 Active IQ Unified Manager 查看灾难恢复设置中的虚拟基础架构可见性 154
配置和管理工作负载 156
在 Active IQ Unified Manager 中配置和管理工作负载 156
工作负载概述 157
管理性能服务级别 162
管理存储效率策略 167
管理和监控 MetroCluster 配置 169
了解 Active IQ Unified Manager 中切换和切回期间的卷行为 169
了解 Active IQ Unified Manager 中基于 FC 的 MetroCluster 配置中的集群连接性 171
了解 Active IQ Unified Manager 中基于 FC 的 MetroCluster 数据镜像 172
在 Active IQ Unified Manager 中监控 MetroCluster 配置 172
在 Active IQ Unified Manager 中监控 MetroCluster 复制 175
管理配额 176
了解 Active IQ Unified Manager 中的配额限制 176
在 Active IQ Unified Manager 中查看用户和用户组配额 176
创建规则以在 Active IQ Unified Manager 中生成电子邮件地址 176
在 Active IQ Unified Manager 中为用户和用户组配额创建电子邮件通知格式 177
在 Active IQ Unified Manager 中编辑用户和组配额电子邮件地址 177
详细了解配额 178
配额对话框的说明 179
故障排除 182
向 Unified Manager 数据库目录添加磁盘空间 182
在 Active IQ Unified Manager 中更改性能统计信息收集间隔 185
更改 Active IQ Unified Manager 保留事件和性能数据的时间长度 186
解决 Active IQ Unified Manager 中的未知身份验证错误 186
解决 Active IQ Unified Manager 中的"用户未找到"错误 187
解决在 Active IQ Unified Manager 中使用其他身份验证服务添加 LDAP 时引起的问题 187
解决 Active IQ Unified Manager 中的 NetApp Manageability SDK 日志轮换问题 188
管理事件和警报 189

管理事件 189
了解 Active IQ Unified Manager 中的 Active IQ 平台事件 189
Event Management System 事件是什么 189
了解 Active IQ Unified Manager 如何处理收到的事件 193
在 Active IQ Unified Manager 中查看事件详细信息 194
在 Active IQ Unified Manager 中查看未分配的事件 195
确认并解决 Active IQ Unified Manager 中的事件 195
在 Active IQ Unified Manager 中将事件分配给特定用户 196
在 Active IQ Unified Manager 中禁用不需要的事件 196
使用 Active IQ Unified Manager 中的自动修复功能修复问题 197
在 Active IQ Unified Manager 中启用和禁用 Active IQ 事件报告 198
在 Active IQ Unified Manager 中上传新的 Active IQ 规则文件 199
Active IQ Unified Manager 如何生成 Active IQ 平台事件 199
在 Active IQ Unified Manager 中解决 Active IQ 平台事件 200
在 Active IQ Unified Manager 中配置事件保留设置 201
什么是 Unified Manager 维护窗口 201
在 Active IQ Unified Manager 中管理主机系统资源事件 203
详细了解事件 204
事件和严重性类型列表 208
事件窗口和对话框说明 251
管理提醒 263
了解 Active IQ Unified Manager 中的警报 263
Active IQ Unified Manager 警报电子邮件中包含的信息 263
添加警报 264
在 Active IQ Unified Manager 中添加性能事件警报 266
在 Active IQ Unified Manager 中测试警报 267
在 Active IQ Unified Manager 中禁用已解决和已过时事件的警报 267
在 Active IQ Unified Manager 中排除灾难恢复目标卷以避免生成警报 268
在 Active IQ Unified Manager 中查看警报 268
在 Active IQ Unified Manager 中编辑警报 269
删除 Active IQ Unified Manager 中的警报 269
警报窗口和对话框的说明 269
管理脚本 275
在 Active IQ Unified Manager 中管理脚本 275
脚本如何与 Active IQ Unified Manager 中的警报配合使用 275
在 Active IQ Unified Manager 中添加脚本 276
删除 Active IQ Unified Manager 中的脚本 277
在 Active IQ Unified Manager 中执行测试脚本 277
了解受支持的 Active IQ Unified Manager CLI 命令 278
脚本窗口和对话框的说明 282
监控和管理集群性能 284

Active IQ Unified Manager 性能监控简介 284
了解 Active IQ Unified Manager 中的性能监控 284
探索 Active IQ Unified Manager 性能监控功能 284
使用 Active IQ Unified Manager 接口管理存储系统性能 285
在 Active IQ Unified Manager 中查看集群配置和性能数据 285
了解 Active IQ Unified Manager 中的数据连续性收集周期 286
了解 Active IQ Unified Manager 中收集的数据和事件中的时间戳 287
在 Unified Manager GUI 中导航性能工作流 287
在 Active IQ Unified Manager GUI 中导航性能工作流 287
登录到 Active IQ Unified Manager UI 287
图形界面和导航路径 288
在 Active IQ Unified Manager 中搜索存储对象 293
在 Active IQ Unified Manager 中筛选清单页面内容 294
从仪表板监控集群性能 295
通过 Active IQ Unified Manager 中的信息板监控集群性能 295
查看 Active IQ Unified Manager 控制面板上的性能面板 296
解释 Active IQ Unified Manager 中的性能横幅消息 296
在 Active IQ Unified Manager 中更改性能统计信息收集间隔 297
使用工作负载分析器排除工作负载故障 297
使用 Active IQ Unified Manager 中的工作负载分析器对工作负载进行故障排除 297
了解 Active IQ Unified Manager 中的工作负载分析器数据 298
了解何时在 Active IQ Unified Manager 中使用工作负载分析器 299
在 Active IQ Unified Manager 中使用工作负载分析器 299
从性能集群登录页面监控集群性能 300
从 Active IQ Unified Manager 的 Performance Cluster Landing 页面监控集群性能 300
了解 Active IQ Unified Manager 中的性能集群登录页面 300
性能集群登录页面 301
使用性能清单页面监控性能 305
使用 Active IQ Unified Manager 中的性能清单页面监控对象性能 305
查看 Active IQ Unified Manager 中所有存储对象的性能清单页面 305
优化性能清单页面内容 310
查看 Active IQ Unified Manager 关于将数据分层到云的建议 312
使用性能资源管理器页面监控性能 313
使用 Active IQ Unified Manager 中的 Performance Explorer 页面监控性能 313
在 Active IQ Unified Manager 中使用根对象进行性能监控 313
筛选 Active IQ Unified Manager 网格中的相关对象 314
指定相关对象的时间范围 314
在 Active IQ Unified Manager 中定义用于比较图形的相关对象 315
了解 Active IQ Unified Manager 中的计数器图表 316
了解 Active IQ Unified Manager 中的性能计数器图表类型 317
选择要在 Active IQ Unified Manager 中显示的性能图表 318

展开 Active IQ Unified Manager 中的计数器图表窗格 319
在 Active IQ Unified Manager 中将计数器图表焦点更改为较短时间段 319
在 Active IQ Unified Manager 事件时间线中查看事件详细信息 319
计数器图表缩放视图 320
在 Active IQ Unified Manager 中按集群组件查看卷延迟 322
在 Active IQ Unified Manager 中按协议查看 SVM IOPS 流量 323
查看卷和 LUN 延迟图表以验证 Active IQ Unified Manager 中的性能保证 323
在 Active IQ Unified Manager 中查看所有 SAN Array 集群的性能 323
在 Active IQ Unified Manager 中查看基于本地工作负载的节点 IOPS 324
对象登录页的组件 325
使用 QoS 策略组信息管理性能 330
使用 Active IQ Unified Manager 中的 QoS 策略组信息管理性能 330
使用 Active IQ Unified Manager 中的存储 QoS 控制工作负载吞吐量 330
查看 Active IQ Unified Manager 上所有集群中可用的 QoS 策略组 331
在 Active IQ Unified Manager 中查看同一 QoS 策略组中的卷或 LUN 331
在 Active IQ Unified Manager 中查看卷或 LUN 的 QoS 策略组设置 332
比较 Active IQ Unified Manager 中同一 QoS 策略组内的卷或 LUN 332
使用 Active IQ Unified Manager 查看吞吐量图表中的 QoS 策略 333
在 Active IQ Unified Manager 中查看工作负载 QoS 最小值和最大值设置 334
使用性能容量和可用 IOPS 信息管理性能 335
在 Active IQ Unified Manager 中管理性能容量和可用 IOPS 335
了解 Active IQ Unified Manager 中已用性能容量计数器 335
使用 Active IQ Unified Manager 中的已用性能容量值 336
了解 Active IQ Unified Manager 中的可用 IOPS 337
在 Active IQ Unified Manager 中查看节点和聚合性能容量使用值 338
查看 Active IQ Unified Manager 中节点和聚合的可用 IOPS 值 339
在 Active IQ Unified Manager 中查看性能容量计数器图表 340
在 Active IQ Unified Manager 中配置已用性能容量阈值 341
使用 Active IQ Unified Manager 中的已用性能容量计数器 342
了解并使用节点故障转移规划页面 342
使用 Active IQ Unified Manager 中的节点故障转移规划页面 342
从 Active IQ Unified Manager 的"性能/节点故障转移规划"页面确定纠正措施 342
查看 Active IQ Unified Manager 中 Performance/Node Failover Planning 页面的组件 343
在 Active IQ Unified Manager 中为节点故障转移规划创建阈值策略 344
在 Active IQ Unified Manager 中使用已用性能容量明细图表进行故障转移规划 344
收集数据并监控工作负载性能 345
在 Active IQ Unified Manager 中收集数据并监控工作负载性能 345
使用 Active IQ Unified Manager 监控工作负载类型 346
了解 Active IQ Unified Manager 中的工作负载性能测量值 347
了解 Active IQ Unified Manager 如何计算预期性能范围 348
使用 Active IQ Unified Manager 中的延迟预测进行性能分析 349

使用工作负载延迟识别 Active IQ Unified Manager 中的性能问题 349
评估集群操作如何影响 Active IQ Unified Manager 中的工作负载延迟 350
使用 Active IQ Unified Manager 监控 MetroCluster 性能 351
了解性能事件和警报 352
了解 Active IQ Unified Manager 中的性能事件和警报 352
确定 Active IQ Unified Manager 中性能事件的来源 352
在 Active IQ Unified Manager 中按严重性对性能事件进行优先级排序 353
监控 Active IQ Unified Manager 检测到的配置更改 353
了解 Active IQ Unified Manager 中系统定义的性能阈值策略 354
分析 Active IQ Unified Manager 中的性能事件和通知 356
了解 Active IQ Unified Manager 如何确定事件的性能影响 358
了解 Active IQ Unified Manager 中的集群组件和争用情况 358
在 Active IQ Unified Manager 中识别性能事件中的工作负载角色 360
管理性能阈值 360
在 Active IQ Unified Manager 中管理性能阈值 360
在 Active IQ Unified Manager 中使用用户定义的性能阈值策略 361
响应 Active IQ Unified Manager 中违反性能阈值策略的问题 362
了解使用 Active IQ Unified Manager 中的阈值跟踪的性能计数器 362
了解 Active IQ Unified Manager 中的组合阈值策略对象和计数器 364
在 Active IQ Unified Manager 中创建用户定义的性能阈值策略 364
在 Active IQ Unified Manager 中为存储对象分配性能阈值策略 365
在 Active IQ Unified Manager 中查看性能阈值策略 366
在 Active IQ Unified Manager 中编辑用户定义的性能阈值策略 367
从 Active IQ Unified Manager 中的存储对象删除性能阈值策略 367
了解 Active IQ Unified Manager 中的性能阈值策略更改 368
在 Active IQ Unified Manager 中移动对象时管理阈值策略 368
分析性能事件 369
分析 Active IQ Unified Manager 中的性能事件 369
在 Active IQ Unified Manager 中显示性能事件信息 369
分析用户定义的性能阈值事件 370
分析系统定义的性能阈值事件 371
分析动态性能阈值事件 375
解决性能事件 382
解决 Active IQ Unified Manager 中的性能事件 382
确认延迟在 Active IQ Unified Manager 中处于预期范围内 382
评估配置更改如何影响 Active IQ Unified Manager 中的工作负载性能 382
通过在 Active IQ Unified Manager 中调整客户端设置来提高工作负载性能 382
了解客户端或网络问题如何影响 Active IQ Unified Manager 中的性能 383
分析 Active IQ Unified Manager 中 QoS 策略组内的高活动量卷 383
移动 LIF 以提高 Active IQ Unified Manager 中的性能 383
在非繁忙时间运行存储效率操作 384

了解添加磁盘如何影响 Active IQ Unified Manager 中的数据重新分配 384
通过在 Active IQ Unified Manager 中的节点上启用 Flash Cache 来提高工作负载性能 385
通过在 Active IQ Unified Manager 上的存储聚合中启用 Flash Pool 来提升工作负载性能 385
在 Active IQ Unified Manager 中检查 MetroCluster 配置运行状况 385
在 Active IQ Unified Manager 中验证 MetroCluster 配置 386
在 Active IQ Unified Manager 中将工作负载移动到不同的聚合 386
将工作负载移动到 Active IQ Unified Manager 中的其他节点 387
在 Active IQ Unified Manager 中将工作负载移至其他节点上的聚合 389
将工作负载移动到 Active IQ Unified Manager 中不同 HA 对的节点 390
将工作负载移动到 Active IQ Unified Manager 中不同 HA 对中的另一个节点 392
使用 QoS 策略设置对 Active IQ Unified Manager 中的节点工作负载进行优先级排序 393
删除 Active IQ Unified Manager 中的非活动卷和 LUN 394
了解添加磁盘如何影响 Active IQ Unified Manager 中的聚合布局 394
在 Unified Manager 服务器和外部数据提供程序之间建立连接 394
在 Active IQ Unified Manager 和外部数据提供程序之间建立连接 395
将 Active IQ Unified Manager 性能数据发送到外部服务器 395
设置 Graphite 以从 Active IQ Unified Manager 接收性能数据 396
配置 Active IQ Unified Manager 与外部数据提供程序之间的连接 396
监控和管理集群运行状况 399
Active IQ Unified Manager 状况监控简介 399
了解 Active IQ Unified Manager 运行状况监控 399
了解Active IQ Unified Manager运行状况监控功能 400
使用 Active IQ Unified Manager 界面管理存储系统运行状况 401
管理和监控集群及集群对象运行状况 401
了解集群监控 401
在 Active IQ Unified Manager 中查看集群列表和详细信息 403
在 Active IQ Unified Manager 中检查 MetroCluster 配置中的集群健康状况 403
在 Active IQ Unified Manager 中查看所有 SAN 阵列集群的运行状况和容量状态 405
在 Active IQ Unified Manager 中查看节点列表和详细信息 406
在 Active IQ Unified Manager 中生成用于合同续签的硬件清单报告 406
在 Active IQ Unified Manager 中查看 Storage VM 列表和详细信息 407
在 Active IQ Unified Manager 中查看聚合列表和详细信息 407
在 Active IQ Unified Manager 中查看 FabricPool 容量信息 408
在 Active IQ Unified Manager 中查看存储池详细信息 409
在 Active IQ Unified Manager 中查看卷列表和详细信息 410
查看 Active IQ Unified Manager 中 NFS 共享的详细信息 410
在 Active IQ Unified Manager 中查看有关 SMB/CIFS 共享的详细信息 411
在 Active IQ Unified Manager 中查看 Snapshot 副本列表 412
在 Active IQ Unified Manager 中删除 Snapshot 副本 412
在 Active IQ Unified Manager 中计算 Snapshot 副本的可回收空间 413
了解 Active IQ Unified Manager 中的集群对象窗口和对话框 413

常见 Unified Manager 运行状况工作流和任务 414
了解常见 Active IQ Unified Manager 运行状况工作流程和任务 414
监控数据可用性并排除故障 415
解决容量问题 421
管理运行状况阈值 422
管理集群安全目标 426
管理备份和还原操作 436
管理脚本 450
管理和监控组 453
使用注释确定存储对象事件的优先级 460
通过 Web UI 和维护控制台发送支持包 468
与多个工作流程相关的任务和信息 474
保护和还原数据 526
创建保护关系并进行故障排除 526
Active IQ Unified Manager 中的 SnapMirror 保护类型 526
在 Unified Manager 中设置保护关系 527
执行保护关系故障转移和故障恢复 529
解决保护作业失败 533
解决 Active IQ Unified Manager 中的滞后问题 536
管理和监控保护关系 537
了解如何在 Active IQ Unified Manager 中管理和监控保护关系 537
在 Active IQ Unified Manager 中查看卷保护状态 537
在 Active IQ Unified Manager 中查看卷保护关系 539
在 Active IQ Unified Manager 中监控一致性组 LUN 关系 540
在 Active IQ Unified Manager 的 Health: All Volumes 视图中创建 SnapVault 关系 540
在 Active IQ Unified Manager 的 Volume/Health 详细信息页面中创建 SnapVault 保护关系 541
在 Active IQ Unified Manager 的 Health: All Volumes 视图中创建 SnapMirror 关系 542
从 Active IQ Unified Manager 中的卷健康状况详细信息页面创建 SnapMirror 关系 543
在 Active IQ Unified Manager 中创建具有版本灵活复制功能的 SnapMirror 关系 544
在 Active IQ Unified Manager 中创建具有版本灵活复制和回退选项功能的 SnapMirror 关系 545
在 Active IQ Unified Manager 中配置目标效率设置 546
在 Active IQ Unified Manager 中创建 SnapMirror 和 SnapVault 计划 547
使用 Active IQ Unified Manager 中的级联或扇出关系扩展保护 547
从 Active IQ Unified Manager 的卷关系页面编辑保护关系 548
从 Active IQ Unified Manager 中的卷/运行状况详细信息页面编辑保护关系 548
创建 SnapMirror 策略以在 Active IQ Unified Manager 中最大化传输效率 549
在 Active IQ Unified Manager 中创建 SnapVault 策略以最大限度地提高传输效率 549
从 Active IQ Unified Manager 的卷关系页面中止传输 550
从 Active IQ Unified Manager 的卷/运行状况详细信息页面中止传输 551
从 Active IQ Unified Manager 的卷关系页面暂停保护关系 551
从 Active IQ Unified Manager 中的卷/运行状况详细信息页面静默保护关系 552

从 Active IQ Unified Manager Volume Relationships 页面中断 SnapMirror 关系 553
从 Active IQ Unified Manager 的卷关系页面删除保护关系 553
从 Active IQ Unified Manager 的卷关系页面恢复已暂停关系上的计划传输 553
从 Active IQ Unified Manager 的"卷/运行状况详细信息"页面恢复已静默关系上的传输 554
从 Active IQ Unified Manager 中的卷关系页面初始化或更新保护关系 555
从 Active IQ Unified Manager 中的卷/运行状况详细信息页面初始化或更新保护关系 555
从 Active IQ Unified Manager 的卷关系页面重新同步保护关系 556
从 Active IQ Unified Manager 的"卷关系"页面反转保护关系 557
使用 Active IQ Unified Manager 中的卷和卷/运行状况详细信息页面还原数据 558
了解 Active IQ Unified Manager 中的资源池 559
在 Active IQ Unified Manager 中创建资源池 560
在 Active IQ Unified Manager 中编辑资源池 560
在 Active IQ Unified Manager 中查看资源池清单 560
在 Active IQ Unified Manager 中添加资源池成员 561
从 Active IQ Unified Manager 的资源池中删除聚合 561
删除 Active IQ Unified Manager 中的资源池 562
监控 Storage VM 灾难恢复保护关系 562
在 Active IQ Unified Manager 中管理 Storage VM 关联 564
支持 Active IQ Unified Manager 中存储服务的 SVM 和资源池要求 566
了解 Active IQ Unified Manager 中的作业 566
监控 Active IQ Unified Manager 中的作业 566
在 Active IQ Unified Manager 中查看作业详细信息 567
在 Active IQ Unified Manager 中中止作业 567
在 Active IQ Unified Manager 中重试失败的保护作业 567
保护关系窗口和对话框说明 568
生成自定义报告 607
Unified Manager 报告 607
了解 Active IQ Unified Manager 报告 607
用于生成报告的访问点 607
了解 Active IQ Unified Manager 中的报告 609
了解 Active IQ Unified Manager 中的视图和报告关系 609
了解 Active IQ Unified Manager 中的报告类型 609
了解 Active IQ Unified Manager 中的报告限制 611
使用报告 611
了解 Active IQ Unified Manager 中的报告工作流 611
开始使用 Active IQ Unified Manager 中的报告功能 612
在 Active IQ Unified Manager 中搜索计划报告 615
自定义报告 615
在 Active IQ Unified Manager 中下载报告 618
计划报告 618
在 Active IQ Unified Manager 中计划报告 618

计划报告 619
管理报告时间表 621
自定义报告示例 623
了解 Active IQ Unified Manager 中的自定义报告示例 623
自定义集群存储报告 623
自定义聚合容量报告 626
自定义卷容量报告 628
自定义 Qtree 容量报告 631
自定义 NFS 共享报告 631
自定义 storage VM 报告 632
自定义卷关系报告 634
自定义卷性能报告 637
Microsoft Excel 报告示例 638
了解 Active IQ Unified Manager 中的 Microsoft Excel 示例报告 638
创建报告以在 Active IQ Unified Manager 中显示聚合容量表和图表 638
在 Active IQ Unified Manager 中显示聚合总容量与可用容量图表 641
创建报告以查看 Active IQ Unified Manager 中的可用卷容量图表 644
创建报告以查看 Active IQ Unified Manager 中可用 IOPS 最多的聚合 646
使用 REST API 管理存储 649
Active IQ Unified Manager 入门 649
Active IQ Unified Manager REST API 入门 649
确定Active IQ Unified Manager REST API的目标用户 649
管理 Active IQ Unified Manager API 访问权限和类别 649
了解 Active IQ Unified Manager 中提供的 REST 服务 650
了解 Active IQ Unified Manager 中的 API 版本号 651
了解 Active IQ Unified Manager 中的 ONTAP 存储资源模型 651
Active IQ Unified Manager 中的 REST API 访问和身份验证 652
在 Active IQ Unified Manager 中访问和验证 REST API 652
了解 Active IQ Unified Manager HTTP 状态代码 655
请遵循使用 Active IQ Unified Manager API 的推荐做法 655
使用 Active IQ Unified Manager 中的系统日志进行故障排除 656
了解 Active IQ Unified Manager 如何使用作业对象进行异步处理 657
了解 Active IQ Unified Manager 中的 Hello API server 示例程序 657
Unified Manager REST API 661
了解 Active IQ Unified Manager REST API 的类别 661
使用 Active IQ Unified Manager 中的 API 管理数据中心中的存储对象 662
通过 Active IQ Unified Manager 中的代理访问来访问 ONTAP API 665
使用 Active IQ Unified Manager 中的 API 执行管理任务 668
使用 API 管理 Active IQ Unified Manager 中的用户 669
使用 Active IQ Unified Manager 中的 API 查看性能指标 669
使用 Active IQ Unified Manager 中的 API 查看作业和系统详细信息 676

使用 Active IQ Unified Manager 中的 API 管理事件和警报 677
管理工作负载 679
存储管理的常见工作流程 686
了解 Active IQ Unified Manager 中用于存储管理的常见 API 工作流 686
使用 Active IQ Unified Manager API 确定聚合中的空间问题 687
使用 Active IQ Unified Manager 事件 API 确定存储对象问题 688
使用 Active IQ Unified Manager 网关 API 对 ONTAP 卷进行故障排除 689
用于工作负载管理的工作流 693
法律声明 716
版权 716
商标 716
专利 716
隐私政策 716
开源 716

Active IQ Unified Manager 文档

Active IQ Unified Manager 发行说明

提供了 Active IQ Unified Manager 9.18 新功能、限制和已知问题的摘要。

有关详细信息，请参见 "Active IQ Unified Manager 发行说明"。

开始使用

在 VMware vSphere 上开始使用 Active IQ Unified Manager

您可以下载包含根证书、 `README` 文件和 `OVA` 文件的 `.tar` 文件，并将 Unified Manager 部署为虚拟设备。

系统要求

- 操作系统：VMware ESXi 8.0
- 内存：12 GB
- CPU：总计 9572 MHz
- 可用磁盘空间：5 GB（精简配置），152 GB（厚配置）

有关详细的系统要求，请参见"安装 Unified Manager 的要求"和"互操作性表"。

安装 Active IQ Unified Manager

下载安装程序

1. 下载包含根证书、 `README` 文件和 `OVA` 文件的 `.tar` 文件。
2. 将文件保存到 vSphere 客户端可访问的本地目录或网络目录。
3. 在下载 `.tar`文件的目录中，输入 `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz`命令。+ 所需的 `OVA` 文件、根证书和 `README`文件将解压到目标目录。

验证完整性

您可以按照 `README`文件中提供的步骤，验证 `OVA`文件的完整性。

安装 **Unified Manager**

1. 在 vSphere 客户端中，单击 文件 **>** 部署 **OVF** 模板。
2. 找到 OVA 文件，然后使用向导在 ESXi 服务器上部署虚拟设备。
3. 在“审阅详细信息”页面的“发布者”部分，消息 `Entrust Code Signing - OVCS2 (Trusted certificate)` 确认了下载的 `OVA`文件的完整性。对于消息 `Entrust Code Signing - OVCS2 (Invalid certificate)`，请将 VMware vCenter Server 升级到 7.0U3E 或更高版本。
4. 在“自定义模板”页面的“属性”选项卡中，根据所执行安装类型的需要填充字段：
   - 对于静态配置，请在所有字段中输入所需信息。无需为 辅助 **DNS** 字段添加信息。
   - 对于使用 IPv4 的 DHCP，请不要在任何字段中添加任何信息。
   - 对于使用 IPv6 的 DHCP，请选中“启用自动 IPv6 寻址”框。请勿在任何其他字段中添加任何信息。
5. 启动此虚拟机。
6. 单击控制台选项卡以查看初始引导过程。

7. 配置时区。
8. 输入 Unified Manager 维护用户名和密码。

安装结束时，将显示连接到 Unified Manager Web UI 的信息。

在 Linux 上开始使用 Active IQ Unified Manager

您可以下载安装包并在物理或虚拟 Red Hat Enterprise Linux 平台上安装 Unified Manager。

系统要求

- 操作系统：Red Hat Enterprise Linux 8.x 和 9.4 版，基于 x86_64 架构，使用操作系统安装程序的 软件选择选项中的“带 GUI 的服务器”基本环境安装
- 内存：12 GB，CPU：总共 9572 MHz
- 可用磁盘空间： `/opt/netapp/data` 目录中有 100 GB 的磁盘空间，根分区中有 50 GB 的磁盘空间。对于单独挂载的 `/opt` 和 `/var/log` 目录，请确保 `/opt` 有 15 GB、 `/var/log` 有 16 GB，以及 `/tmp` 有 10 GB 的可用空间。

有关详细系统要求以及在安全站点中安装产品的信息，请参见 "安装 Unified Manager 的要求" 和 "互操作性表"。

安装 Active IQ Unified Manager

下载安装程序

1. 下载 `ActiveIQUnifiedManager-<version>.zip`安装包以及代码签名证书(.pem`）和数字签名(`.sig`）。
2. 在已下载安装文件的目录中，运行：

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

验证完整性

运行以下命令以验证安装程序包的完整性：

- 运行 `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>` 以从代码签名证书创建包含公钥的文件。
- 运行 `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip`以验证安装程序包上的签名。

验证存储库配置

配置 Red Hat Enterprise Linux 存储库的过程因站点而异。您可以使用安装包中包含的 `pre_install_check.sh` 脚本来验证操作系统的配置。如果您的系统已连接到 Internet，您将自动收到设置 Red Hat Enterprise Linux 存储库的说明。

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

安装 **Unified Manager**

Unified Manager 使用 `yum` 实用程序安装软件和任何相关软件。由于 Red Hat Enterprise Linux 的映像各不相同，因此安装的程序包取决于映像中存在的软件。该 `yum` 实用程序确定要安装的依赖软件包。如果需要有关依赖软件包的更多信息，请参见 "Linux 软件和安装要求"。

要安装 Unified Manager，请以 root 用户身份或使用 `sudo`，从解压安装文件的目录中运行以下命令：

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

或

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

在安装结束时，将显示连接到 Unified Manager Web UI 的信息。如果您无法连接到 Web UI，请参阅随软件提供的 `README`文件，了解有关端口 443 限制的更多信息。

在 **Windows** 上开始使用 **Active IQ Unified Manager**

您可以下载安装包并安装 Unified Manager，以监控和排除数据存储容量、可用性、性能和保护问题。

系统要求

- 操作系统
  - Microsoft Windows Server 2019 标准版和数据中心版
  - Microsoft Windows Server 2022 标准版和数据中心版

    Unified Manager 在 64 位 Windows 操作系统上支持以下语言：

  - 英语
  - 日语
  - 简体中文
- 内存：12 GB
- CPU：总计 9572 MHz
- 可用磁盘空间：安装目录 100 GB 磁盘空间，MySQL 数据目录 50 GB 磁盘空间

有关详细的系统要求，请参见"安装 Unified Manager 的要求"和"互操作性表"。

安装 **Active IQ Unified Manager**

下载安装程序

1. 下载 `ActiveIQUnifiedManager-<version>.exe` 安装包。
2. 将安装文件复制到目标系统上的目录。

安装 **Unified Manager**

要安装 Unified Manager，请确保已安装 Microsoft .NET 4.5.2 或更高版本。作为安装过程的一部分，Unified Manager 将根据需要安装其他第三方软件包。有关依赖软件包的详细信息，请参见 "Windows 软件和安装要求"。

1. 使用默认本地管理员帐户登录到 Windows。
2. 在下载安装文件的目录中，右键单击并以管理员身份运行 Unified Manager 可执行文件（.exe）。
3. 出现提示时，输入用户名和密码以创建 Unified Manager 维护用户。
4. 在数据库连接向导中，输入 MySQL root 密码。
5. 按照其余提示完成安装。
6. 在安装结束时单击 完成，将显示 Unified Manager Web UI。

在 VMware vSphere 系统上安装 Unified Manager

了解Active IQ Unified Manager

了解Active IQ Unified Manager

Active IQ Unified Manager（以前称为 OnCommand Unified Manager）使您能够从单个界面监控和管理 ONTAP 存储系统的运行状况和性能。您可以在 Linux 服务器、Windows 服务器或 VMware 主机上作为虚拟应用装置部署 Unified Manager。

完成安装并添加要管理的集群后，Unified Manager 将提供显示受监视存储系统的容量、可用性、保护和性能状态的图形界面。

相关信息

"NetApp 互操作性表工具"

了解 Active IQ Unified Manager 服务器的作用

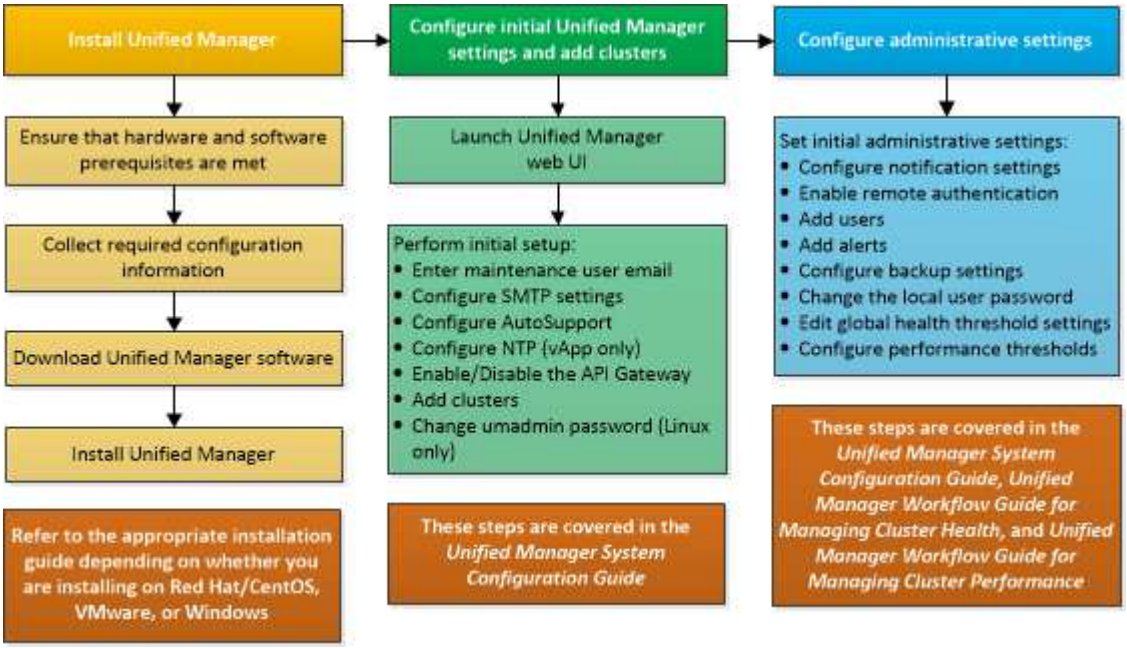
Unified Manager 服务器基础架构由数据收集单元、数据库和应用程序服务器组成。它提供基础架构服务，例如发现、监视、基于角色的访问控制（RBAC）、审核和记录。

Unified Manager 收集群集信息，将数据存储在数据库中，并分析数据以查看是否存在任何群集问题。

了解 Active IQ Unified Manager 安装顺序

安装工作流描述了在使用 Unified Manager 之前必须执行的任务。

这些部分介绍了以下工作流程中显示的每个项目。



安装 Unified Manager 的要求

确保服务器满足 Active IQ Unified Manager 安装要求

在开始安装过程之前，请确保要安装 Unified Manager 的服务器满足特定的软件、硬件、CPU 和内存要求。

NetApp 不支持对 Unified Manager 应用程序代码进行任何修改。如果需要对 Unified Manager 服务器应用任何安全措施，则应对安装 Unified Manager 的操作系统进行这些更改。

有关将安全措施应用于 Unified Manager 服务器的详细信息，请参见知识库文章。

"应用于 Active IQ Unified Manager for Clustered Data ONTAP 的安全措施的可支持性"

相关信息

有关详细信息，请参见 "NetApp 互操作性表工具"

了解 Active IQ Unified Manager 的虚拟基础架构和硬件要求

在虚拟基础架构或物理系统上安装 Unified Manager 应满足内存、CPU 和磁盘空间的最低要求。

下表显示了建议的内存、CPU 和磁盘空间资源值。这些值已经过验证，以确保 Unified Manager 达到可接受的性能水平。

硬件配置	建议的设置
RAM	12 GB
处理器	4 个 CPU
CPU 周期容量	总共 9572 MHz（最低要求 9572 MHz）
可用磁盘空间	• 5 GB （精简配置） • 152 GB（厚配置）

Unified Manager 可以安装在内存较小的系统上，但建议使用 12 GB RAM，以确保有足够的内存来实现最佳性能，并使系统能够在配置增长时容纳更多的集群和存储对象。您不应在部署 Unified Manager 的虚拟机上设置任何内存限制，也不应启用任何阻碍软件利用系统上分配的内存的功能（例如内存气球机制）。

此外，在安装 Unified Manager 的第二个实例之前，Unified Manager 的单个实例可以监视的节点数是有限制的。有关节点限制、CPU 和内存建议，请参阅 "Unified Manager 最佳实践指南"。

内存页面交换会对系统和管理应用程序的性能产生负面影响。竞争由于整体主机利用率而无法使用的 CPU 资源可能会降低性能。

专用要求

安装 Unified Manager 的物理或虚拟系统应专门用于 Unified Manager，不应与其他应用程序共享。其他应用程序可能会消耗系统资源，并可能大幅降低 Unified Manager 的性能。

备份的空间要求

如果您计划使用 Unified Manager 备份和还原功能，请分配额外的容量，以便“`data`”目录或磁盘具有 150 GB 的空间。备份可以写入本地目标或远程目标。最佳做法是确定 Unified Manager 主机系统外部具有至少 150 GB 空间的远程位置。

主机连接要求

安装 Unified Manager 的物理系统或虚拟系统应进行相应配置，以便您可以从主机本身成功 `ping`主机名。如果是 IPv6 配置，您应验证对主机名的 `ping6`是否成功，以确保 Unified Manager 安装成功。

您可以使用主机名（或主机 IP 地址）访问产品 Web UI。如果在部署期间为网络配置了静态 IP 地址，则您已为网络主机指定了名称。如果使用 DHCP 配置了网络，则应从 DNS 获取主机名。

如果您计划允许用户使用短名称而不是使用完全限定的域名（FQDN）或 IP 地址来访问 Unified Manager，则您的网络配置必须将此短名称解析为有效的 FQDN。

了解 **Active IQ Unified Manager** 的 **VMware** 软件和安装要求

安装 Unified Manager 的 VMware vSphere 系统需要特定版本的操作系统和特定版本的支持软件。

操作系统软件

支持的操作系统是 VMware ESXi 8.0。

> VMware vSphere 系统上的 Unified Manager OVA 在内部运行 Debian OS 13 (Trixie)。有关受支持版本的 ESXi 服务器可以支持的虚拟机硬件版本的信息，请参见 VMware 文档。

支持以下版本的 vSphere：

- VMware vCenter Server 7.0 和 8.0

有关受支持的 ESXi 版本的完整和最新列表，请参见互操作性列表。

"mysupport.netapp.com/cn/matrix"

为了使虚拟设备正常运行，VMware ESXi 服务器时间应与 NTP 服务器时间相同。将 VMware ESXi 服务器时间与 NTP 服务器时间同步可防止时间故障。

安装要求

支持 Unified Manager 虚拟应用装置的 VMware High Availability。

如果在运行 ONTAP 软件的存储系统上部署 NFS 数据存储，请使用适用于 VMware VAAI 的 NetApp NFS 插件来使用厚配置。

如果由于资源不足而导致使用启用了高可用性的环境部署失败，您可能需要通过禁用 VM 重新启动优先级并保持主机隔离响应处于开启状态，来修改群集功能虚拟机选项。

> 在安装或升级 Unified Manager 时，所需的第三方软件和安全修补程序会自动安装或升级到

VMware vSphere 系统上。由于 Unified Manager 安装和升级过程控制这些组件，因此不应尝试独立安装或升级任何第三方组件。

在 **Active IQ Unified Manager** 中使用受支持的浏览器

要访问 Unified Manager Web UI，请使用受支持的浏览器。

互操作性矩阵包含支持的浏览器版本列表。

"mysupport.netapp.com/cn/matrix"

对于所有浏览器，禁用弹出窗口拦截器可确保正确显示软件功能。

如果您计划为 SAML 身份验证配置 Unified Manager，以便身份提供程序（IdP）可以对用户进行身份验证，则还应检查 IdP 支持的浏览器列表。

了解 **Active IQ Unified Manager** 的协议和端口要求

所需的端口和协议支持 Unified Manager 服务器与托管存储系统、服务器和其他组件之间的通信。

到 **Unified Manager** 服务器的连接

在典型安装中，连接到 Unified Manager Web UI 时不必指定端口号，因为始终使用默认端口。例如，由于 Unified Manager 始终尝试在其默认端口上运行，因此您可以输入 `https://<host>`而不是 `https://<host>:443`。

Unified Manager 服务器使用特定协议访问以下接口：

接口	协议	端口	问题描述
Unified Manager Web UI	HTTP	80	用于访问 Unified Manager Web UI；自动重定向到安全端口 443。
Unified Manager Web UI 和使用 API 的程序	HTTPS	443	用于安全地访问 Unified Manager Web UI 或进行 API 调用；只能使用 HTTPS 进行 API 调用。
维护控制台	SSH/SFTP	22	用于访问维护控制台并检索支持包。
Linux 命令行	SSH/SFTP	22	用于访问 Red Hat Enterprise Linux 命令行并检索支持捆绑包。
系统日志	UDP	514	用于从 ONTAP 系统访问基于订阅的 EMS 消息，并根据这些消息创建事件。

接口	协议	端口	问题描述
REST	HTTPS	9443	用于从经过身份验证的 ONTAP 系统访问基于实时 REST API 的 EMS 事件。
MySQL 数据库	MySQL	3306	用于启用 OnCommand Workflow Automation 和 OnCommand API Services 对 Unified Manager 的访问。
AMQP QPID 代理	TCP/IP	56072	用于内部消息通信。
AMQP QPID 代理	WebSocket over TCP	56080	用于在此端口上侦听从 ONTAP（云代理）接收的消息。
AMQP QPID 代理	WebSocket over TCP	56443	用于在此端口上侦听从 ONTAP（云代理）接收的消息。此端口上的通信支持 TLS 或 SSL 提供的加密。

在 VMware vSphere 系统上安装 Unified Manager 时，MySQL 的默认端口 3306 仅限于 localhost。这不会影响任何升级场景，在这些场景中会保留先前的配置。可以修改此配置，并且可以使用维护控制台上的 `Control access to MySQL port 3306` 选项使其他主机能够建立连接。有关信息，请参见 "其他菜单选项"。可以使用 Unified Manager 维护控制台更改用于 HTTP 和 HTTPS 通信的端口（端口 80 和 443）。有关详细信息，请参见 "维护控制台菜单"。

来自 **Unified Manager** 服务器的连接

您应将防火墙配置为打开端口，以启用 Unified Manager 服务器与受管存储系统、服务器和其他组件之间的通信。如果端口未打开，则通信失败。

根据您的环境，可以选择修改 Unified Manager 服务器用于连接到特定目标的端口和协议。

Unified Manager 服务器使用以下协议和端口连接到托管存储系统、服务器和其他组件：

目标	协议	端口	问题描述
存储系统	HTTPS	443/TCP	用于监控和管理存储系统。 如果要使用此端口或任何其他端口连接到 VMware vCenter Server 或 ESXi 服务器，请确保端口可用并且可以在安全站点中连接。
存储系统	NDMP	10000/TCP	用于某些 Snapshot 还原操作。
AutoSupport 服务器	HTTPS	443	用于发送 AutoSupport 信息。需要互联网访问才能执行此功能。
身份验证服务器	LDAP	389	用于发出身份验证请求以及用户和组查找请求。
LDAPS	636	用于安全 LDAP 通信。	邮件服务器
SMTP	25	用于发送警报通知电子邮件。	SNMP 陷阱发送方
SNMPv1 或 SNMPv3	162/UDP	用于发送警报通知 SNMP 陷阱。	外部数据提供程序服务器
TCP	2003	用于将性能数据发送到外部数据提供程序，例如 Graphite。	NTP 服务器
NTP	123/UDP	用于将 Unified Manager 服务器上的时间与外部 NTP 时间服务器同步。（仅限 VMware 系统）	AMQP QPID 代理
TCP/IP	56072	用于内部消息通信。	AMQP QPID 代理
WebSocket over TCP	56080	用于在此端口上侦听从 ONTAP（云代理）接收的消息。	AMQP QPID 代理
WebSocket over TCP	56443	用于在此端口上侦听从 ONTAP（云代理）接收的消息。此端口上的通信支持 TLS 或 SSL 提供的加密。	系统日志

在 **Active IQ Unified Manager** 中填写工作表

在安装和配置 Unified Manager 之前，应准备好有关环境的特定信息。您可以在工作表中记录信息。

Unified Manager 安装信息

安装 Unified Manager 所需的详细信息。

部署软件的系统	您的价值
ESXi 服务器 IP 地址	
主机完全限定的域名	
主机 IP 地址	
网络掩码	
网关 IP 地址	
主 DNS 地址	
辅助 DNS 地址	
搜索域	
维护用户名	
维护用户密码	

Unified Manager 配置信息

安装后配置 Unified Manager 的详细信息。某些值是可选的，具体取决于您的配置。

设置	您的价值
维护用户电子邮件地址	
NTP 服务器	
SMTP 服务器主机名或 IP 地址	
SMTP 用户名	
SMTP 密码	
SMTP 端口	25（默认值）
发送警报通知的电子邮件	
身份验证服务器主机名或 IP 地址	
Active Directory 管理员名称或 LDAP 绑定可分辨名称	
Active Directory 密码或 LDAP 绑定密码	
身份验证服务器基本可分辨名称	
身份提供程序（IdP）URL	
身份提供程序（IdP）元数据	

设置	您的价值
SNMP 陷阱目标主机 IP 地址	
SNMP 端口	

集群信息

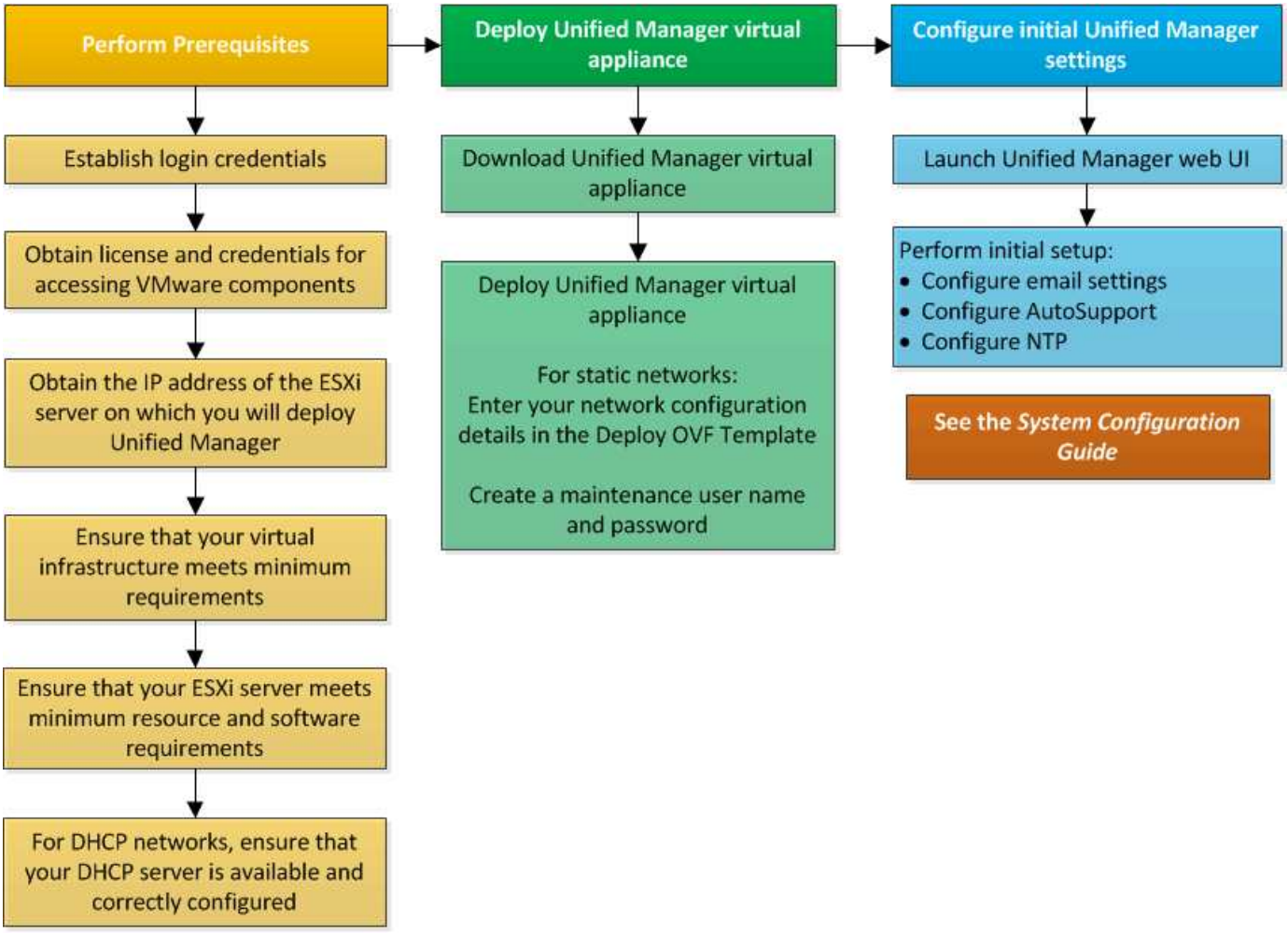
使用 Unified Manager 管理的存储系统的详细信息。

第 **1** 个集群，共 **N** 个	您的价值
主机名或集群管理 IP 地址	
ONTAP 管理员用户名 必须为管理员分配“admin”角色。	
ONTAP 管理员密码	
协议	HTTPS

在 VMware vSphere 上安装、升级和删除 Unified Manager

了解 Active IQ Unified Manager 部署流程

部署工作流描述了在使用 Unified Manager 之前必须执行的任务。



Unified Manager 虚拟设备部署工作流

部署 **Active IQ Unified Manager**

部署 Unified Manager 包括下载软件、部署虚拟设备、创建维护用户名和密码以及在 Web UI 中执行初始设置。

开始之前

- 您应验证并完成部署的系统要求。

  请参阅 "系统要求"。

- 请确保您有下列信息：
  - NetApp 支持站点的登录凭据
  - 用于访问 VMware vCenter Server 和 vSphere Web Client 的凭据
  - 要在其上部署 Unified Manager 虚拟应用装置的 ESXi 服务器的 IP 地址
  - 有关数据中心的详细信息，例如数据存储中的存储空间和内存要求
  - 如果您计划使用 IPv6 寻址，则应在主机上启用 IPv6。

您可以将 Unified Manager 部署为 VMware ESXi 服务器上的虚拟设备。

您应该使用 VMware 控制台访问维护控制台，而不是使用 SSH。

> 从 Unified Manager 9.8 开始，VMware Tools 已替换为 Open VM Tools `open-vm-tools`）。您不再需要在安装过程中安装 VMware Tools，因为 `open-vm-tools`包含在 Unified Manager 安装包中。

完成部署和初始设置后，您可以添加集群，或者在维护控制台中配置其他网络设置，然后访问 web UI。

步骤

1. 按照"下载 Unified Manager"中的步骤进行操作。
2. 此外，请按照 "部署 Unified Manager 虚拟设备" 中的步骤进行操作。

下载 **Active IQ Unified Manager** 安装文件

从 NetApp 支持站点下载 Unified Manager 安装文件，以将 Unified Manager 部署为虚拟设备。

开始之前

您应该拥有 NetApp 支持站点的登录凭据。

安装文件是一个 `.tar`文件，其中包含根证书、一个 `README`文件以及一个包含为虚拟设备配置的 Unified Manager 软件的 `OVA`文件。

步骤

1. 登录到 NetApp 支持站点，然后导航到 Unified Manager 的下载页面：

   "NetApp 支持站点"

2. 选择所需的 Unified Manager 版本并接受最终用户许可协议（EULA）。
3. 下载 VMware vSphere 安装 `.tar`文件并将其保存到 vSphere Client 可访问的本地目录或网络目录。
4. 验证校验和，以确保软件正确下载。
5. 导航到下载 `.tar` 文件的目录，并在终端窗口中输入以下命令以展开 Unified Manager 捆绑包：

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

   将 Unified Manager 的所需 `OVA`文件、根证书和一个 `README`文件解压缩到目标目录。

6. 按照 `README`文件中提供的步骤，验证 `OVA`文件的完整性。

部署 **Active IQ Unified Manager** 虚拟设备

下载安装文件后，将 Unified Manager 部署为虚拟设备。使用 vSphere Web 客户端在 ESXi 服务器上部署虚拟设备。部署虚拟设备时，将创建一个虚拟机。

开始之前

您应该查看系统要求。在部署 Unified Manager 虚拟设备之前进行必要的更改。

请参阅 "虚拟基础架构要求"。

请参阅 "VMware 软件和安装要求"。

如果使用动态主机配置协议（DHCP），请确保 DHCP 服务器可用，并且 DHCP 和虚拟机（VM）网络适配器配置正确。默认情况下已配置 DHCP。

如果使用静态网络配置，请确保 IP 地址未在同一子网中重复，并且已配置相应的 DNS 服务器条目。

在部署虚拟设备之前获取以下信息：

- 用于访问 VMware vCenter Server 和 vSphere Web Client 的凭据
- 要在其上部署 Unified Manager 虚拟应用装置的 ESXi 服务器的 IP 地址
- 数据中心的详细信息，例如存储空间的可用性
- 如果您不使用 DHCP，请获取您计划连接的网络设备的 IPv4 或 IPv6 地址：
  - 主机的完全限定域名（FQDN）
  - 主机的 IP 地址
  - 网络掩码
  - 默认网关的 IP 地址
  - 主 DNS 地址和辅助 DNS 地址
  - 搜索域

从 Unified Manager 9.8 开始，VMware Tools 已替换为 Open VM Tools `open-vm-tools`）。您不必在安装过程中安装 VMware Tools，因为 `*open-vm-tools*`已包含在 Unified Manager 安装包中。

部署虚拟应用装置时，将生成用于 HTTPS 访问的唯一自签名证书。访问 Unified Manager Web UI 时，您可能会看到有关不可信证书的浏览器警告。

支持 Unified Manager 虚拟应用装置的 VMware High Availability。

步骤

1. 在 vSphere 客户端中，单击 文件 > 部署 **OVF** 模板。
2. 完成部署 OVF 模板向导以部署 Unified Manager 虚拟设备。

   在“审阅详细信息”页面上：

   - 请验证 Publisher 部分的详细信息。消息 **Entrust Code Signing - OVCS2** （可信证书） 确认了下载的 `OVA`文件的完整性。+ 如果您看到消息 **Entrust Code Signing - OVCS2** （无效证书），请将 VMware vCenter Server 升级到 7.0U3E 或更高版本。

     在“自定义模板”页面上：

   - 使用 DHCP 和 IPv4 寻址时，将所有字段留空。
   - 选中 “启用自动 IPv6 寻址” 复选框，并在使用 DHCP 和 IPv6 寻址时将所有其他字段留空。
   - 如果要使用静态网络配置，可以填写此页面上的字段，这些设置将在部署期间应用。请确保 IP 地址对于其部署所在的主机是唯一的，尚未使用，并且具有有效的 DNS 条目。

3. 将 Unified Manager 虚拟设备部署到 ESXi 服务器后，通过右键单击 VM，然后选择 **Power On** 来打开 VM 电源。

   如果开机操作因资源不足而失败，请添加资源，然后重试安装。

4. 单击 **Console** 选项卡。

   初始启动过程需要几分钟才能完成。

5. 要配置您的时区，请按照 VM 控制台窗口中的提示输入您的地理区域以及您的城市或地区。

   无论受管设备上的时区设置如何，显示的所有日期信息都使用为 Unified Manager 配置的时区。如果您的存储系统和管理服务器配置了相同的 NTP 服务器，则即使它们显示的时间不同，它们也指向同一时间点。例如，如果您使用配置了与管理服务器不同时区的设备创建 Snapshot 副本，则时间戳为管理服务器的时间。

6. 如果没有可用的 DHCP 服务，或者静态网络配置的详细信息中有错误，请选择以下选项之一：

使用的协议	操作
DHCP	选择 重试 **DHCP**。如果您计划使用 DHCP，则应确保配置正确。 如果使用启用了 DHCP 的网络，则会自动将 FQDN 和 DNS 服务器条目提供给虚拟设备。如果未使用 DNS 正确配置 DHCP，则会自动分配主机名“UnifiedManager”，并将其与安全证书关联。如果尚未设置已启用 DHCP 的网络，则应手动输入网络配置信息。
静态网络配置	a. 选择*输入静态网络配置的详细信息*。 配置过程需要几分钟才能完成。 b. 确认您输入的值，然后选择 **Y**。

7. 在提示符处输入维护用户名，然后单击 **Enter**。

   维护用户名应以 a-z 中的字母开头，后跟 -、a-z 或 0-9 的任意组合。

8. 在提示符处输入密码，然后单击 **Enter**。

   VM 控制台显示 Unified Manager Web UI 的 URL。

您可以访问 Web UI 以执行 Unified Manager 的初始设置，如 "配置 Active IQ Unified Manager" 中所述。

Unified Manager 虚拟设备升级工作流

升级 Active IQ Unified Manager

您只能从 9.14 或 9.16 版本将 Active IQ Unified Manager 升级到 9.18 版本。

在升级过程中，Unified Manager 不可用。在升级 Unified Manager 之前，您应完成所有正在运行的操作。

如果 Unified Manager 与 OnCommand Workflow Automation 实例配对，并且这两种产品都有可用的新版本软件，则必须断开这两种产品的连接，然后在执行升级后设置新的 Workflow Automation 连接。如果您仅对其中一款产品执行升级，则应在升级后登录 Workflow Automation，并验证其是否仍在从 Unified Manager 获取数据。

如果您的系统从 Unified Manager 9.7 升级，由于 Debian 版本中的文件系统更改，您无法直接从 9.14 升级到 9.18。请改为遵循以下推荐的升级路径：9.14 → 9.16P2 → 9.18。

步骤

1. 按照"下载 Unified Manager ISO 映像"中的步骤进行操作。
2. 此外，请按照 "升级 Unified Manager" 中所述的步骤进行操作。

请对 **Active IQ Unified Manager** 版本使用受支持的升级路径

Active IQ Unified Manager 支持每个版本的特定升级路径。

并非所有版本的 Unified Manager 都可以就地升级到更高版本。Unified Manager 升级仅限于 N-2 模式。这意味着您只能在所有平台上升级到接下来的两个版本。例如，您只能从 Unified Manager 9.14 和 9.16 升级到 Unified Manager 9.18。

如果运行的版本早于受支持的版本，则需要先将 Unified Manager 实例升级到受支持的版本之一，然后再升级到当前版本。

例如，如果安装的版本是 Unified Manager 9.9，并且要升级到 Unified Manager 9.14，则需要执行一系列升级。

升级路径示例：

1. 升级 9.11 → 9.13
2. 升级 9.13 → 9.14
3. 升级 9.13 → 9.16
4. 升级 9.14 或 9.16 → 9.18

有关升级路径矩阵的更多信息，请参见此 "知识库（KB）文章"。

下载 **Active IQ Unified Manager** 升级文件

在升级 Unified Manager 之前，请从 NetApp 支持站点下载 Unified Manager 升级文件。

开始之前

您应该拥有 NetApp 支持站点的登录凭据。

步骤

1. 登录到 NetApp 支持站点：

   "NetApp 支持站点"

2. 导航到下载页面以升级 VMware vSphere 上的 Unified Manager。
3. 请下载要升级的 `.iso`映像，并将其保存到您的 vSphere Client 可访问的本地目录或网络目录。

4. 验证校验和，以确保软件已正确下载。

升级 **Active IQ Unified Manager** 虚拟设备

您可以将 Active IQ Unified Manager 虚拟设备从版本 9.14 或 9.16 升级到 9.18。

开始之前

确保以下内容：

- 您已从 NetApp 支持站点下载升级文件，即 ISO 映像。
- 您要升级 Unified Manager 的系统满足系统和软件要求。

  请参阅 "虚拟基础架构要求"。

  请参阅 "VMware 软件和安装要求"。

- 对于 vSphere 6.5 及更高版本的用户，您已安装 VMware 远程控制台（VMRC）。
- 在升级期间，系统可能会提示您确认是要将先前保留性能数据的默认设置保留 13 个月，还是将其更改为 6 个月。确认后，6 个月后将清除历史性能数据。
- 您有下列信息：
  - NetApp 支持站点的登录凭据
  - 用于访问 VMware vCenter Server 和 vSphere Web Client 的凭据
  - Unified Manager 维护用户的凭据

在升级过程中，Unified Manager 不可用。在升级 Unified Manager 之前，您应完成所有正在运行的操作。

如果您已将 Workflow Automation 和 Unified Manager 配对，则应手动更新 Workflow Automation 中的主机名。

步骤

1. 在 vSphere 客户端中，单击 主页 > 清单 > 虚拟机和模板。
2. 选择安装了 Unified Manager 虚拟设备的虚拟机（VM）。
3. 如果 Unified Manager VM 正在运行，请导航到 摘要 > 命令 > 关闭来宾。
4. 创建 Unified Manager 虚拟机的备份副本（如快照或克隆），以创建应用程序一致性备份。
5. 从 vSphere 客户端启动 Unified Manager 虚拟机。
6. 启动 VMware 远程控制台。
7. 单击 **CDROM** 图标，然后选择 连接到磁盘映像文件（**.iso**）。
8. 选择 `ActiveIQUnifiedManager-<version>-virtual-update.iso`文件，然后单击*打开*。
9. 单击 **Console** 选项卡。
10. 登录到 Unified Manager 维护控制台。
11. 在主菜单中，选择*升级*。

    此时将显示一条消息，提示 Unified Manager 在升级过程中不可用，并在完成后恢复。

12. 键入 `y`以继续。

    系统将显示警告，提醒您备份虚拟设备所在的虚拟机。

13. 键入 `y`以继续。

    升级过程和重新启动 Unified Manager 服务可能需要几分钟才能完成。

14. 按任意键继续。

    您已自动注销维护控制台。

15. 可选： 登录到维护控制台，并验证 Unified Manager 的版本。

您可以在受支持的 Web 浏览器上的新窗口中启动 Web UI，然后登录以使用 Unified Manager 的升级版本。请注意，您需要等待发现过程完成后才能在 UI 中执行任何任务。

重新启动 **Active IQ Unified Manager** 虚拟机

您可以从维护控制台重新启动 Unified Manager 虚拟机（VM）。在生成新的安全证书后，或者虚拟机出现问题时，您应重新启动虚拟机。

开始之前

- 应打开虚拟设备的电源。
- 您应以维护用户身份登录到 Unified Manager 维护控制台。

您还可以使用 VMware **Restart Guest** 选项从 vSphere 重新启动虚拟机。请参阅 "Broadcom 的 VMware vSphere PowerCLI CMDLET 参考中的 Restart-VMGuest cmdlet。"

步骤

1. 在维护控制台中，选择*系统配置* > 重新启动虚拟机。
2. 从浏览器启动 Unified Manager Web UI，然后登录。

删除 **Active IQ Unified Manager**

您可以通过删除安装了 Unified Manager 软件的虚拟机（VM）来卸载 Unified Manager。

开始之前

- 您应具有访问 VMware vCenter Server 和 vSphere Web Client 的凭据。
- 应关闭 Unified Manager 服务器到 Workflow Automation 服务器的任何活动连接。
- 在删除虚拟机（VM）之前，应从 Unified Manager 服务器中删除所有集群（数据源）。

步骤

1. 请使用 Unified Manager 维护控制台验证 Unified Manager 服务器没有到外部数据提供程序的活动连接。
2. 在 vSphere 客户端中，单击 主页 > 清单 > 虚拟机和模板。
3. 选择要删除的虚拟机，然后单击*摘要*选项卡。

4. 如果虚拟机正在运行，请单击*电源* > 关闭客户机。
5. 右键单击要删除的虚拟机，然后单击*从磁盘删除*。

在 Linux 系统上安装 Unified Manager

Active IQ Unified Manager 简介

了解Active IQ Unified Manager

Active IQ Unified Manager（以前称为 OnCommand Unified Manager）使您能够从单个界面监控和管理 ONTAP 存储系统的运行状况和性能。您可以在 Linux 服务器、Windows 服务器或 VMware 主机上作为虚拟应用装置（vApp）部署 Unified Manager。

完成安装并添加要管理的集群后，Unified Manager 将提供显示受监视存储系统的容量、可用性、保护和性能状态的图形界面。

相关信息

"NetApp 互操作性表工具"

了解 Active IQ Unified Manager 服务器的作用

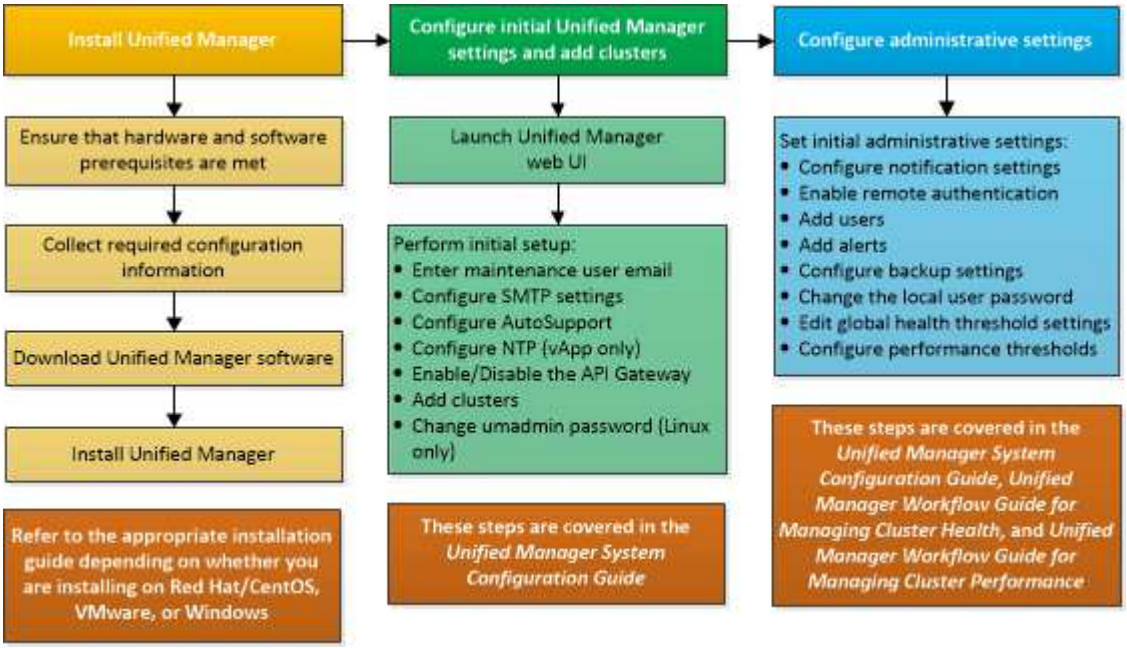
Unified Manager 服务器基础架构由数据收集单元、数据库和应用程序服务器组成。它提供基础架构服务，例如发现、监视、基于角色的访问控制（RBAC）、审核和记录。

Unified Manager 收集群集信息，将数据存储在数据库中，并分析数据以查看是否存在任何群集问题。

查看 Active IQ Unified Manager 的安装顺序

安装工作流描述了在使用 Unified Manager 之前必须执行的任务。

这些部分介绍了以下工作流程中显示的每个项目。



安装 Unified Manager 的要求

了解安装 Active IQ Unified Manager 的要求

在开始安装过程之前，请确保要安装 Unified Manager 的服务器满足特定的软件、硬件、CPU 和内存要求。

NetApp 不支持对 Unified Manager 应用程序代码进行任何修改。如果需要对 Unified Manager 服务器应用任何安全措施，则应对安装 Unified Manager 的操作系统进行这些更改。

有关将安全措施应用于 Unified Manager 服务器的详细信息，请参见知识库文章。

"应用于 Active IQ Unified Manager for Clustered Data ONTAP 的安全措施的可支持性"

相关信息

"NetApp 互操作性表工具"

了解 Active IQ Unified Manager 的虚拟基础架构和硬件要求

在虚拟基础架构或物理系统上安装 Unified Manager 应满足内存、CPU 和磁盘空间的最低要求。

下表显示了建议的内存、CPU 和磁盘空间资源值。这些值已经过验证，以确保 Unified Manager 达到可接受的性能水平。

硬件配置	建议的设置
RAM	12 GB
处理器	4 个 CPU
CPU 周期容量	总共 9572 MHz（最低要求 9572 MHz）
可用磁盘空间	150 GB，其中容量分配如下： • 分配给根分区 50 GB • 分配给 `/opt/netapp/data` 目录的 100 GB 可用磁盘空间，该目录挂载在 LVM 驱动器或连接到目标系统的单独本地磁盘上 对于单独挂载的 `/opt`和 `/var/log`目录，请确保 `/opt`有 15 GB 可用空间，且 `/var/log`有 16 GB 可用空间。 `/tmp`目录应至少有 10 GB 可用空间。

Unified Manager 可以安装在内存较小的系统上，但建议使用 12 GB RAM，以确保有足够的内存来实现最佳性能，并使系统能够在配置增长时容纳更多的集群和存储对象。您不应在部署 Unified Manager 的虚拟机上设置任何内存限制，也不应启用任何阻碍软件利用系统上分配的内存的功能（例如内存气球机制）。

此外，在安装 Unified Manager 的第二个实例之前，Unified Manager 的单个实例可以监视的节点数是有限制

的。有关节点限制、CPU 和内存建议，请参见 "《Unified Manager 最佳实践指南》"。

内存页面交换会对系统和管理应用程序的性能产生负面影响。竞争由于整体主机利用率而无法使用的 CPU 资源可能会降低性能。

专用要求

安装 Unified Manager 的物理或虚拟系统应专门用于 Unified Manager，不应与其他应用程序共享。其他应用程序可能会消耗系统资源，并可能大幅降低 Unified Manager 的性能。

备份的空间要求

如果您计划使用 Unified Manager 备份和还原功能，请分配额外的容量，以便“`data`”目录或磁盘具有 150 GB 的空间。备份可以写入本地目标或远程目标。最佳做法是确定 Unified Manager 主机系统外部具有至少 150 GB 空间的远程位置。

主机连接要求

安装 Unified Manager 的物理系统或虚拟系统应进行相应配置，以便您可以从主机本身成功 `ping`主机名。如果是 IPv6 配置，您应验证对主机名的 `ping6`是否成功，以确保 Unified Manager 安装成功。

您可以使用主机名（或主机 IP 地址）访问产品 Web UI。如果在部署期间为网络配置了静态 IP 地址，则您已为网络主机指定了名称。如果使用 DHCP 配置了网络，则应从 DNS 获取主机名。

如果您计划允许用户使用短名称而不是使用完全限定的域名（FQDN）或 IP 地址来访问 Unified Manager，则您的网络配置必须将此短名称解析为有效的 FQDN。

了解 **Active IQ Unified Manager** 中的 **Linux** 软件和安装要求

安装 Unified Manager 的 Linux 系统需要特定版本的操作系统和支持软件。对于 Linux 安装，只能在 Red Hat Enterprise Linux 操作系统上安装 Unified Manager。它不能安装在任何其他操作系统上。

操作系统软件

Linux 系统必须安装下列版本的操作系统和支持软件：

- Red Hat Enterprise Linux 8.x 和 9.6 版，基于 x86_64 架构

有关受支持的 Red Hat Enterprise Linux 版本的完整和最新列表，请参阅互操作性矩阵。

"NetApp 互操作性矩阵"

服务器应专用于运行 Unified Manager。不应在服务器上安装其他应用程序。在某些环境中，由于公司策略，已在 Linux 系统上安装 Qualys 等漏洞扫描程序。您应在安装 Unified Manager 之前禁用漏洞扫描程序，以防止安装失败。

在内部（Unified Manager 和漏洞扫描程序安装在同一台虚拟机上）或外部（Unified Manager 和漏洞扫描程序安装在两台不同的服务器上，漏洞扫描程序扫描安装了 Unified Manager 的虚拟机）扫描虚拟机（VM）时，漏洞扫描程序（如 Qualys）可能会导致高 CPU 使用率。此问题通常会导致虚拟机无响应并影响 Unified Manager 服务。因此，NetApp 建议在安装了 Unified Manager

的虚拟机中禁用漏洞扫描程序。如果无法禁用扫描程序，请在非营业时间扫描虚拟机，并在扫描完成后重新启动服务。

第三方软件

Unified Manager 部署在 WildFly Web 服务器上。WildFly 27.0.1.Final 与 Unified Manager 捆绑并配置。

需要以下第三方软件包，但未包含在 Unified Manager 中。如果您已按照以下各节所述配置了存储库，则在安装过程中， `yum` 安装程序会自动安装这些软件包。

- MySQL Community Edition 版本 8.4.10（来自 MySQL 存储库）
- OpenJDK 版本 17.0.14+6（来自 Red Hat Extra Enterprise Linux Server 存储库）
- Python 3.13.3 （来自 Red Hat Extra Enterprise Linux Server 存储库）
- 7zip 版本 7z2301-linux-x64。有关详细信息，请查看 "配置 7-zip 软件包"。

在升级任何第三方软件之前，必须关闭正在运行的 Unified Manager 实例。第三方软件安装完成后，您可以重新启动 Unified Manager。

用户授权要求

在 Linux 系统上安装 Unified Manager 可以由 root 用户或非 root 用户使用 `sudo`命令执行。

此外，默认的 Unified Manager 安装会在 `/etc/sudoers.d/` 目录的 sudoers 文件 (`ocum_sudoers` 和 `ocie_sudoers`）中包含 umadmin 用户（默认维护用户）和 jboss 用户。如果由于安全策略或安全监控工具而从您的环境中删除了此内容，则必须将其重新添加回来。您需要保留 sudoers 配置，因为某些 Unified Manager 操作需要这些 sudo 权限。

安装要求

下面列出了在系统上安装 Red Hat Enterprise Linux 和相关存储库的最佳实践。以不同方式安装或配置的系统，或异地部署（在云中）的系统可能需要其他步骤，并且 Unified Manager 可能无法在此类部署中正常运行。

- 您必须根据 Red Hat 最佳实践安装 Red Hat Enterprise Linux，并且应选择以下默认选项，这需要选择“Server with GUI” 基本环境。
- 在 Red Hat Enterprise Linux 上安装 Unified Manager 时，系统必须能够访问相应的存储库，以便安装程序可以访问和安装所有必需的软件依赖项。
- 要使 `yum`安装程序在 Red Hat Enterprise Linux 存储库中查找依赖软件，必须在安装 Red Hat Enterprise Linux 期间或之后使用有效的 Red Hat 订阅注册系统。

  有关 Red Hat Subscription Manager 的信息，请参见 Red Hat 文档。

- 必须启用 Extra Packages for Enterprise Linux （EPEL） 存储库，才能在系统上成功安装所需的第三方实用程序。

  如果未在系统上配置 EPEL 存储库，则必须手动下载并配置存储库。

  请参阅 "手动配置 EPEL 存储库"。

- 如果未安装正确版本的 MySQL，则必须启用 MySQL 存储库才能在系统上成功安装 MySQL 软件。

如果未在系统上配置 MySQL 存储库，则必须手动下载并配置存储库。

请参阅 "手动配置 MySQL 存储库"。

- 只能在 Unified Manager 主机上安装一个版本的 Java；否则，系统可能无法确定要使用的版本。请参阅 "在 Active IQ Unified Manager 主机上更新 Java 后，服务将无法启动"。

如果您的系统没有互联网访问权限，并且存储库未从连接互联网的系统镜像到未连接的系统，则应按照安装说明确定系统的外部软件依赖关系。然后，您可以将所需的软件下载到连接互联网的系统，并将 `.rpm`文件复制到计划安装 Unified Manager 的系统。要下载工件和软件包，必须使用 `yum install`命令。您必须确保两个系统运行相同的操作系统版本，并且订阅许可证适用于相应的 Red Hat Enterprise Linux。

您不得从此处列出的存储库以外的存储库安装所需的第三方软件。从 Red Hat 存储库安装的软件专为 Red Hat Enterprise Linux 设计，并符合 Red Hat 最佳实践（目录布局、权限等）。来自其他位置的软件可能不遵守这些准则，这可能会导致 Unified Manager 安装失败，或可能导致未来升级出现问题。

端口 **443** 要求

Red Hat Enterprise Linux 的通用映像可能会阻止对端口 443 的外部访问。由于此限制，安装 Unified Manager 后，您可能无法连接到管理员 Web UI。运行以下命令允许通用 Red Hat Enterprise Linux 上的所有外部用户和应用程序访问端口 443。

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

必须使用“`Server with GUI`”基本环境安装 Red Hat Enterprise Linux。它提供了 Unified Manager 安装说明使用的命令。其他基本环境可能需要您安装其他命令以验证或完成安装。如果系统上 `firewall-cmd` 不可用，则必须通过运行以下命令进行安装：

```
# sudo yum install firewalld
```

请在运行命令之前联系您的 IT 部门，以查看您的安全策略是否需要不同的流程。

应在 Red Hat 系统上禁用 THP（Transparent Huge Pages）。启用后，在某些情况下，当某些进程占用过多内存并被终止时，可能会导致 Unified Manager 关闭。

请使用支持的浏览器访问 **Active IQ Unified Manager**

要访问 Unified Manager Web UI，请使用受支持的浏览器。

互操作性矩阵包含支持的浏览器版本列表。

"mysupport.netapp.com/cn/matrix"

对于所有浏览器，禁用弹出窗口拦截器可确保正确显示软件功能。

如果您计划为 SAML 身份验证配置 Unified Manager，以便身份提供程序（IdP）可以对用户进行身份验证，则还应检查 IdP 支持的浏览器列表。

了解 **Active IQ Unified Manager** 中的协议和端口要求

所需的端口和协议支持 Unified Manager 服务器与托管存储系统、服务器和其他组件之间的通信。

到 **Unified Manager** 服务器的连接

在典型安装中，连接到 Unified Manager Web UI 时不必指定端口号，因为始终使用默认端口。例如，由于 Unified Manager 始终尝试在其默认端口上运行，因此您可以输入 `https://<host>`而不是 `https://<host>:443`。

Unified Manager 服务器使用特定协议访问以下接口：

接口	协议	端口	问题描述
Unified Manager Web UI	HTTP	80	用于访问 Unified Manager Web UI；自动重定向到安全端口 443。
Unified Manager Web UI 和使用 API 的程序	HTTPS	443	用于安全地访问 Unified Manager Web UI 或进行 API 调用；只能使用 HTTPS 进行 API 调用。
维护控制台	SSH/SFTP	22	用于访问维护控制台并检索支持包。
Linux 命令行	SSH/SFTP	22	用于访问 Red Hat Enterprise Linux 命令行并检索支持捆绑包。
MySQL 数据库	MySQL	3306	用于启用 OnCommand Workflow Automation 和 OnCommand API Services 对 Unified Manager 的访问。
系统日志	UDP	514	用于从 ONTAP 系统访问基于订阅的 EMS 消息，并根据这些消息创建事件。
REST	HTTPS	9443	用于从经过身份验证的 ONTAP 系统访问基于实时 REST API 的 EMS 事件。
MySQL 数据库	MySQL	3306	用于启用 OnCommand Workflow Automation 和 OnCommand API Services 对 Unified Manager 的访问。
AMQP QPID 代理	TCP/IP	56072	用于内部消息通信。
AMQP QPID 代理	WebSocket over TCP	56080	用于在此端口上侦听从 ONTAP（云代理）接收的消息。

接口	协议	端口	问题描述
AMQP QPID 代理	WebSocket over TCP	56443	用于在此端口上侦听从 ONTAP（云代理）接收的消息。此端口上的通信支持 TLS 或 SSL 提供的加密。

在 Linux 系统上安装 Unified Manager 时，MySQL 的默认端口 3306 仅限于本地主机。这不会影响保留先前配置的任何升级场景。此配置可以修改，并且可以通过使用维护控制台上的 `Control access to MySQL port 3306`选项将连接提供给其他主机。有关信息，请参见"其他菜单选项"。可以使用 Unified Manager 维护控制台更改用于 HTTP 和 HTTPS 通信的端口（端口 80 和 443）。有关详细信息，请参见"维护控制台菜单"。

来自 **Unified Manager** 服务器的连接

您应将防火墙配置为打开端口，以启用 Unified Manager 服务器与受管存储系统、服务器和其他组件之间的通信。如果端口未打开，则通信失败。

根据您的环境，可以选择修改 Unified Manager 服务器用于连接到特定目标的端口和协议。

Unified Manager 服务器使用以下协议和端口连接到托管存储系统、服务器和其他组件：

目标	协议	端口	问题描述
存储系统	HTTPS	443/TCP	用于监控和管理存储系统。
存储系统	NDMP	10000/TCP	用于某些 Snapshot 还原操作。
AutoSupport 服务器	HTTPS	443	用于发送 AutoSupport 信息。需要互联网访问才能执行此功能。
身份验证服务器	LDAP	389	用于发出身份验证请求以及用户和组查找请求。
LDAPS	636	用于安全 LDAP 通信。	邮件服务器
SMTP	25	用于发送警报通知电子邮件。	SNMP 陷阱发送方
SNMPv1 或 SNMPv3	162/UDP	用于发送警报通知 SNMP 陷阱。	外部数据提供程序服务器
TCP	2003	用于将性能数据发送到外部数据提供程序，例如 Graphite。	NTP 服务器
NTP	123/UDP	用于将 Unified Manager 服务器上的时间与外部 NTP 时间服务器同步。（仅限 VMware 系统）	系统日志

目标	协议	端口	问题描述
UDP	514	由 Unified Manager 用于将审核日志发送到远程 syslog 服务器。	AMQP QPID 代理
TCP/IP	56072	用于内部消息通信。	AMQP QPID 代理
WebSocket over TCP	56080	用于在此端口上侦听从 ONTAP（云代理）接收的消息。	AMQP QPID 代理

在 **Active IQ Unified Manager** 中填写工作表

在安装和配置 Unified Manager 之前，应准备好有关环境的特定信息。您可以在工作表中记录信息。

Unified Manager 安装信息

安装 Unified Manager 所需的详细信息。

部署软件的系统	您的价值
主机完全限定的域名	
主机 IP 地址	
网络掩码	
网关 IP 地址	
主 DNS 地址	
辅助 DNS 地址	
搜索域	
维护用户名	
维护用户密码	

Unified Manager 配置信息

安装后配置 Unified Manager 的详细信息。某些值是可选的，具体取决于您的配置。

设置	您的价值
维护用户电子邮件地址	
SMTP 服务器主机名或 IP 地址	
SMTP 用户名	
SMTP 密码	
SMTP 端口	25（默认值）
发送警报通知的电子邮件	

设置	您的价值
身份验证服务器主机名或 IP 地址	
Active Directory 管理员名称或 LDAP 绑定可分辨名称	
Active Directory 密码或 LDAP 绑定密码	
身份验证服务器基本可分辨名称	
身份提供程序（IdP）URL	
身份提供程序（IdP）元数据	
SNMP 陷阱目标主机 IP 地址	
SNMP 端口	

集群信息

使用 Unified Manager 管理的存储系统的详细信息。

第 **1** 个集群，共 **N** 个	您的价值
主机名或集群管理 IP 地址	
ONTAP 管理员用户名 必须为管理员分配“admin”角色。	
ONTAP 管理员密码	
协议	HTTPS

安装、升级和删除 **Unified Manager** 软件

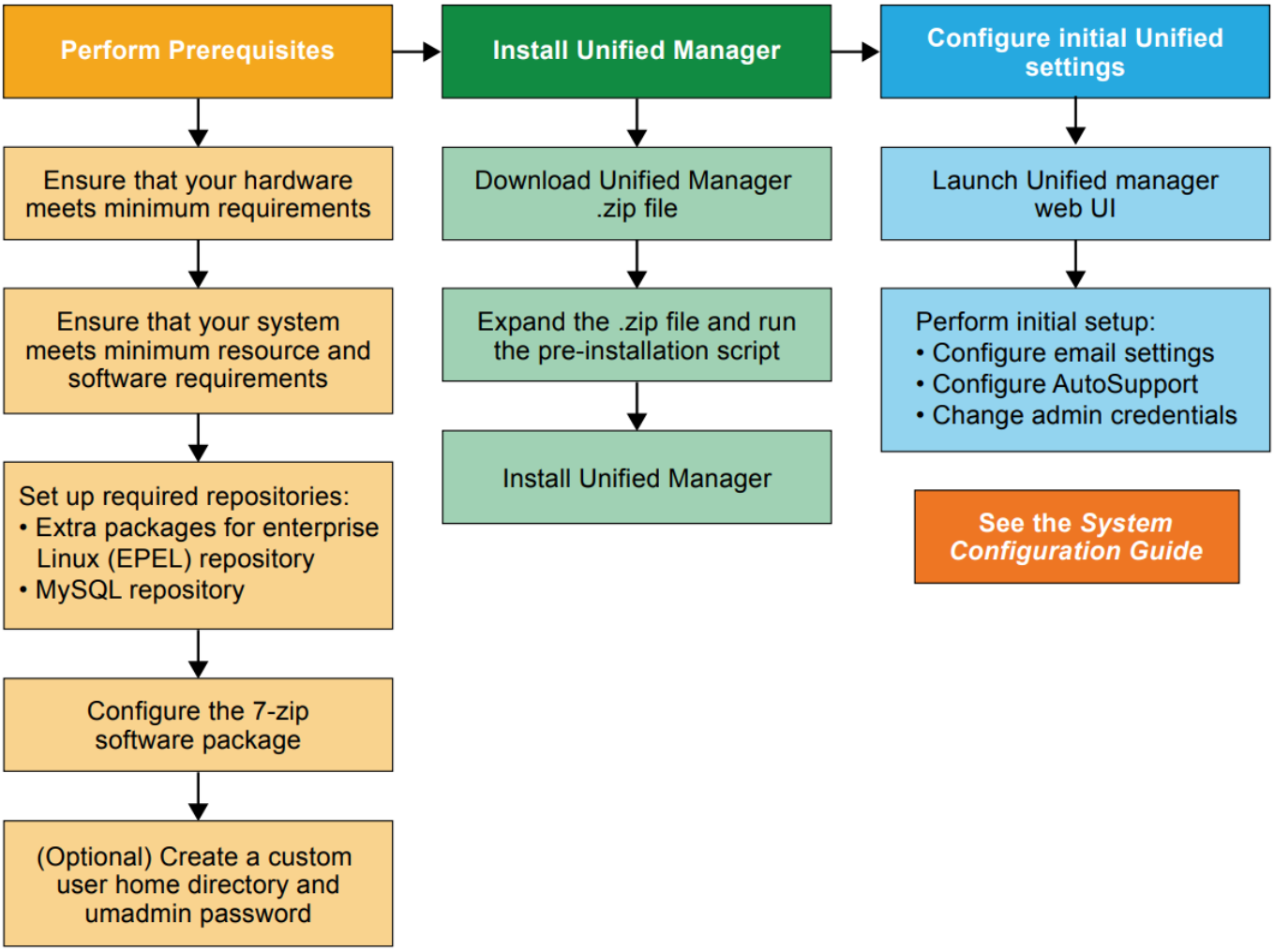
安装、升级和删除 **Active IQ Unified Manager** 软件

在 Linux 系统上，您可以安装 Unified Manager 软件、升级到较新版本的软件或删除 Unified Manager。

Unified Manager 可以安装在 Red Hat Enterprise Linux 服务器上。安装 Unified Manager 的 Linux 服务器可以运行在物理机上，也可以运行在基于 VMware ESXi、Microsoft Hyper-V 或 Citrix XenServer 的虚拟机上。

了解在 **Red Hat Enterprise Linux** 上安装 **Active IQ Unified Manager** 的顺序

安装工作流描述了在使用 Unified Manager 之前必须执行的任务。



设置所需的软件

为 **Active IQ Unified Manager** 配置 **EPEL** 存储库

如果要安装 Unified Manager 的系统无权访问 Extra Packages for Enterprise Linux (EPEL) 存储库，则必须手动下载并配置该存储库以成功安装。

EPEL 存储库提供对必须安装在系统上的所需第三方实用程序的访问权限。您可以使用 EPEL 存储库在 Red Hat Enterprise Linux 系统上安装 Unified Manager。

步骤

1. 下载适用于您安装环境的 EPEL 存储库。对于版本 8，请从以下位置下载：

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

   对于版本 9，请从以下位置下载：

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

2. 配置 EPEL 存储库：

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

对于 Red Hat Enterprise Linux 8 系统，如果您有包含模块化 RPM 软件包的内部存储库，例如 *javapackages-filesystem-<version>.module.rpm*，请确保模块化软件包的元数据在同一存储库中也可用。

配置 **Active IQ Unified Manager** 的 **MySQL** 存储库

如果要安装 Unified Manager 的系统无权访问 MySQL Community Edition 存储库，则必须手动下载并配置存储库以成功安装。

MySQL 存储库提供对必须安装在系统上的所需 MySQL 软件的访问权限。

如果系统没有互联网连接，此任务可能会失败。如果要安装 Unified Manager 的系统没有互联网访问权限，请参阅 MySQL 文档。

步骤

1. 为您的安装下载适当的 MySQL 存储库。对于版本 8，请从以下位置下载：

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

   对于版本 9，请从以下位置下载：

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

2. 配置 MySQL 存储库：

   ```
   yum install mysql84-community-release-.noarch.rpm
   ```

对于 Red Hat Enterprise Linux 8 系统，如果您有包含 java-17-openjdk、7-zip 以及由 AppStream 存储库提供的其他软件包的内部存储库，则必须禁用您的 AppStream 存储库并安装 MySQL Community Server。运行以下命令：

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

如果您收到缺少密钥或密钥不匹配的错误，并且安装失败，请尝试以下步骤：

- 在连接的系统上，通过运行以下命令导入更新的 MySQL 密钥：

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

for example:

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

- 在没有互联网连接的系统上，更新您的 MySQL repo 文件并通过标记 `gpgcheck=0`来禁用 `gpgcheck`。

在 **Active IQ Unified Manager** 中配置 **7-zip** 软件包

要在 Red Hat Enterprise Linux 系统上成功安装 Unified Manager，您的系统必须设置为具有 7-zip 软件包的访问权限。如果网络访问可用并且 7-zip URL 未被防火墙阻止，则在安装或升级过程中，7-zip 会自动下载到您的系统。NetApp 建议使用自动下载方法。

确保在防火墙中取消阻止以下 URL，以允许 Unified Manager 自动下载 7-zip 软件包：
https://7-zip.org/a/7z2301-linux-x64.tar.xz

或者，您可以预安装 7-zip。

预先安装 **7-zip** 软件包

您可以通过手动下载或使用捆绑脚本预安装 7-zip。从以下两种方法中选择一种：

使用捆绑脚本下载

步骤

1. 运行 Unified Manager zip 文件中包含的 `install7zip.sh`脚本。

手动下载

请确保您仅从官方网站下载 7-zip 压缩包。

步骤

1. 从官方网站下载 7-zip 包（版本 23.01）：

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

2. 将文件复制到您的 RHEL 虚拟机：

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

3. 解压归档文件：

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

4. 将 `7zz`文件移动到 `/usr/bin/`目录：

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

5. 设置可执行权限：

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

验证安装

验证您的系统是否已成功安装 7-zip 软件包：

```
7zz -version
```

在 Active IQ Unified Manager 中为 NFS 和 CIFS 共享配置 SELinux

如果您计划在 NAS 或 SAN 设备上挂载 /opt/netapp`或 `/opt/netapp/data，并且启用了 SELinux，则需要注意一些注意事项。

如果您计划从根文件系统以外的任何位置挂载 /opt/netapp`或 `/opt/netapp/data，并且您的环境中已启用 SELinux，则应为挂载的目录设置正确的上下文。对于环境中适用的场景，请按照以下步骤设置和确认正确的 SELinux 上下文。

挂载 `/opt/netapp/data`时配置 SELinux 上下文

如果您已在系统中挂载了 /opt/netapp/data`且 SELinux 设置为 `Enforcing，请确保将 /opt/netapp/data`的 SELinux 上下文类型设置为 `mysqld_db_t，这是数据库文件位置的默认上下文元素。

1. 运行此命令来检查上下文：

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

   输出示例：

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

   在此输出中，上下文是 default_t。应将此上下文更改为 mysqld_db_t。

2. 执行这些步骤，根据您的挂载方式设置上下文 /opt/netapp/data。

   a. 运行以下命令以将上下文设置为 mysqld_db_t：
   ```
   semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"
   `restorecon -R -v /opt/netapp/data
   ```

   b. 如果您已在 /etc/fstab`中配置了 `/opt/netapp/data，则应编辑 `/etc/fstab`文件。对于 `/opt/netapp/data/`挂载选项，请按如下所示添加 MySQL 标签：

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

   c. 卸载并重新挂载 `/opt/netapp/data/`以启用上下文。

d. 如果您有直接 NFS 装载，请运行以下命令将上下文设置为 `mysqld_db_t`：

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

3. 验证上下文设置是否正确：

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

输出示例：

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

在挂载 **`/opt/netapp`**并且也单独挂载 **`/opt/netapp/data/`**时配置 **SELinux** 上下文

在此方案中，首先，您应该按照上一节所述为 `/opt/netapp/data/`设置上下文。在为 `/opt/netapp/data/`设置正确的上下文之后，请确保父目录 `/opt/netapp`未将 `SELinux` 上下文设置为 `file_t`。

步骤

1. 运行此命令来检查上下文：

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

   输出示例：

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

   在此输出中，上下文为 `file_t`，应予以更改。以下命令将上下文设置为 `usr_t`。您可以根据安全要求将上下文设置为 `file_t`以外的任何值。

2. 根据您挂载 `/opt/netapp`的方式，执行以下步骤来设置上下文。

   a. 运行以下命令以设置上下文：

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

1. 如果您已在 `/etc/fstab`中配置了 `/opt/netapp`，则应编辑 `/etc/fstab`文件。对于 `/opt/netapp`挂载选项，请按如下方式添加 MySQL 标签：

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

2. 卸载，然后再次挂载 `/opt/netapp`以启用上下文。
3. 如果您有直接 NFS 挂载，请运行以下命令来设置上下文：

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

a. 验证上下文设置是否正确：

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

示例输出

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

在挂载 `/opt/netapp`且未单独挂载 `/opt/netapp/data/`时配置 SELinux 上下文

如果您已在系统中装载了 /opt/netapp`并且 SELinux 设置为 `Enforcing，请确保将 /opt/netapp`的 SELinux 上下文类型设置为 `mysqld_db_t，这是数据库文件位置的默认上下文元素。

步骤

1. 运行此命令来检查上下文：

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

输出示例：

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

在此输出中，上下文是 default_t。应将此上下文更改为 mysqld_db_t。

2. 请执行以下步骤，根据您装载 `/opt/netapp`的方式设置上下文。

a. 运行以下命令以将上下文设置为 mysqld_db_t：
```
semanage fcontext -a -t mysqld_db_t "/opt/netapp"
`restorecon -R -v /opt/netapp
```

b. 如果您已在 /etc/fstab`中配置了 `/opt/netapp，请编辑 /etc/fstab`文件。对于 `/opt/netapp/`挂载选项，请按如下方式添加 MySQL 标签：
`context=system_u:object_r:mysqld_db_t:s0

c. 卸载，然后再次挂载 `/opt/netapp/`以启用上下文。

d. 如果具有直接 NFS 装载，请运行以下命令将上下文设置为 mysqld_db_t：
```
mount <nfsshare>:/<mountpoint> /opt/netapp -o
context=system_u:object_r:mysqld_db_t:s0
```

3. 验证上下文设置是否正确：

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

输出示例：

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

在 Linux 系统上安装 Unified Manager

在安装 **Active IQ Unified Manager** 之前，创建自定义用户主目录和 **umadmin** 密码

在安装 Unified Manager 之前，您可以创建自定义主目录并定义自己的 umadmin 用户密码。此任务是可选的，但某些站点可能需要这种灵活性来覆盖 Unified Manager 安装默认设置。

开始之前

- 系统必须满足 "硬件系统要求" 中所述的要求。
- 您必须能够以 root 用户身份登录到 Red Hat Enterprise Linux 系统。

默认的 Unified Manager 安装执行以下任务：

- 创建 umadmin 用户，并将 `/home/umadmin`作为主目录。
- 为 umadmin 用户分配默认密码“admin”。

由于某些安装环境会限制对 `/home`的访问，因此安装失败。您必须在其他位置创建主目录。此外，某些站点可能具有有关密码复杂性的规则，或者要求密码由本地管理员设置，而不是由安装程序设置。

如果您的安装环境要求覆盖这些安装默认设置，请按照以下步骤创建自定义主目录并定义 umadmin 用户的密码。

在安装之前定义此信息时，安装脚本将发现这些设置并使用定义的值，而不是使用安装默认设置。

此外，默认的 Unified Manager 安装会将 umadmin 用户包含在 sudoers 文件（(`ocum_sudoers` 和 `ocie_sudoers`）的 `/etc/sudoers.d/` 目录中。如果由于安全策略或某些安全监控工具而从环境中删除此内容，则必须将其重新添加回来。您需要保留 sudoers 配置，因为某些 Unified Manager 操作需要这些 sudo 权限。

环境中的安全策略不得限制 Unified Manager 维护用户的 sudo 权限。如果权限受限，某些 Unified Manager 操作可能会失败。验证成功安装后以 umadmin 用户身份登录时是否能够运行以下 sudo 命令。

```
sudo systemctl status ocie
```

此命令应返回 ocie 服务的适当状态，没有任何错误。

步骤

1. 以 root 用户身份登录到服务器。
2. 创建名为 “maintenance” 的 umadmin 组帐户：

   ```
   groupadd maintenance
   ```

3. 在您选择的主目录下的维护组中创建用户帐户“`umadmin`”：

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

4. 定义 umadmin 密码：

```
passwd umadmin
```

系统提示您输入 umadmin 用户的新密码字符串。

安装 Unified Manager 后，您必须指定 umadmin 用户登录 shell。

下载 **Active IQ Unified Manager**

您必须从 NetApp 支持站点下载 Unified Manager `.zip` 文件才能安装 Unified Manager。

开始之前

您必须具有 NetApp 支持站点的登录凭据。

您下载适用于 Red Hat Enterprise Linux 系统的 Unified Manager 安装包。

步骤

1. 登录到 NetApp 支持站点，然后导航到 Unified Manager 的下载页面：

   "NetApp 支持站点"

2. 选择所需的 Unified Manager 版本并接受最终用户许可协议（EULA）。
3. 下载适用于 Linux 的 Unified Manager 安装程序文件，并将该 `.zip`文件保存到目标系统上的目录中。

   - 请确保为您的 Red Hat Enterprise Linux 系统下载正确版本的安装程序文件。根据您安装的是 Red Hat Enterprise Linux 8 还是 9，请确保下载相应版本的 Unified Manager `.zip` 文件。
   - NetApp 建议您下载代码签名证书 (`.pem`) 和数字签名 (`.sig`) ，以及 `.zip` 文件。

4. 验证校验和以确保已下载软件的完整性。
5. 如果您已下载代码签名证书和数字签名，则可以验证安装程序文件的完整性。您可以使用以下命令来验证安装程序文件的完整性：
   - 此命令将创建一个包含代码签名证书公钥的文件：

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

     - 其中 **AIQUM-RHEL-CLIENT-INTER-ROOT.pem** 是包含代码签名证书的文件。
   - 此命令验证安装程序文件上的签名：

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

类似于 `Verified Ok`的消息确认安装程序文件可以安全使用。

在 **Red Hat Enterprise Linux** 上安装 **Active IQ Unified Manager**

您可以在物理或虚拟 Red Hat Enterprise Linux 平台上安装 Unified Manager。

开始之前

- 要安装 Unified Manager 的系统必须满足系统和软件要求。

  请参阅 "硬件系统要求"。

  请参阅 "Linux 软件和安装要求"。

- 您必须已将 Unified Manager `.zip` 文件从 NetApp 支持站点下载到目标系统。
- 您应该已经验证了下载的 `.zip`文件的完整性。
- 您必须具有受支持的 Web 浏览器。
- 您的终端仿真软件必须启用滚动回退。

Red Hat Enterprise Linux 系统可能安装了所需支持软件的所有所需版本（Java、MySQL、其他实用程序），仅安装了某些所需软件，或者可能是未安装任何所需软件的新安装系统。

步骤

1. 登录到要安装 Unified Manager 的服务器。
2. 输入适当的命令来评估哪些软件可能需要在目标系统上安装或升级以支持安装：

所需软件和最低版本	用于验证软件和版本的命令
OpenJDK 版本 17.0.14+6	`java -version`
MySQL 8.4.10 社区版	`rpm -qa
grep -i mysql`	7-zip

3. 如果安装的 MySQL 版本早于 MySQL 8.4.10 Community Edition，请输入以下命令进行卸载：

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

   如果收到依赖关系错误，则必须添加 `--nodeps` 选项以卸载组件。

4. 导航到下载安装 `.zip`文件的目录并展开 Unified Manager 捆绑包：

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

   Unified Manager 所需的 `.rpm`模块已解压缩到目标目录。

5. 验证目录中是否存在以下模块：

   ```
   ls *.rpm
   ```

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

6. 运行预安装脚本，以确保没有可能与 Unified Manager 安装冲突的系统配置设置或任何已安装的软件：

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

   预安装脚本检查系统是否具有有效的 Red Hat Enterprise Linux 订阅，以及是否可以访问所需的软件存储库。如果脚本发现任何问题，您必须在安装 Unified Manager 之前修复这些问题。

   对于 Red Hat Enterprise Linux 8 系统，如果您的内部存储库包含 JDK 17 - OpenJDK、7-zip 和 AppStream 存储库提供的其他软件包，则必须禁用 AppStream 存储库并安装 MySQL Community Server。运行以下命令：

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

7. *可选：*仅当您的系统未连接到互联网并且必须手动下载安装所需的软件包时，才必须执行第 7 步。如果您的系统可以访问互联网，并且所有必需的软件包都可用，请转至第 8 步。对于未连接到互联网或未使用 Red Hat Enterprise Linux 存储库的系统，请执行以下步骤来确定是否缺少任何所需的软件包，然后下载这些软件包：

   a. 在安装 Unified Manager 的系统上，查看可用和不可用软件包的列表：+
      `yum install netapp-um<version>.x86_64.rpm --assumeno`

      “`Installing:`”部分中的项目是当前目录中可用的包，而“`Installing for dependencies:`”部分中的项目是系统中缺少的包。

   b. 在可以访问互联网的系统上，下载缺失的软件包：

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

      由于插件 “yum-plugin-downloadonly” 在 Red Hat Enterprise Linux 系统上并不总是启用，因此您可能需要启用该功能以下载软件包而不安装它：
      `yum install yum-plugin-downloadonly`

   a. 将缺失的软件包从已连接互联网的系统复制到您的安装系统。

8. 作为 root 用户，或者使用 `sudo`，运行以下命令来安装软件：

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

   此命令将安装 .rpm 软件包、所有其他必要的支持软件以及 Unified Manager 软件。

   如果安装失败并显示 GPG NOKEY 错误，请使用 `rpm --import` 从 URL 导入密钥：

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

   请勿尝试使用其他命令（例如 `rpm -ivh`）进行安装。在 Red Hat Enterprise Linux 系统上成功安装 Unified Manager 需要将所有 Unified Manager 文件和相关文件按特定顺序安装到特定目录结构中，该结构由 `yum install netapp-um<version>.x86_64.rpm` 命令自动执行。

9. 忽略安装消息后立即显示的电子邮件通知。

   该电子邮件会通知 root 用户初始 cron 作业失败，这对安装没有任何不良影响。

10. 安装消息完成后，向上滚动查看消息，直到看到系统显示 Unified Manager Web UI 的 IP 地址或 URL、维护用户名 （umadmin） 以及默认密码的消息。

    此消息与以下内容类似：

    ```
    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. 记录 IP 地址或 URL、分配的用户名（umadmin）和当前密码。

12. 如果在安装 Unified Manager 之前使用自定义主目录创建了 umadmin 用户帐户，则必须指定 umadmin 用户登录 shell：

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

访问 Web UI 以更改 umadmin 用户的默认密码，并执行 Unified Manager 的初始设置，如 "配置 Active IQ Unified Manager" 中所述。必须更改 umadmin 用户的默认密码。

了解 **Active IQ Unified Manager** 安装期间创建的用户

在 Red Hat Enterprise Linux 上安装 Unified Manager 时，Unified Manager 和第三方实用程序将创建以下用户：umadmin、jboss 和 mysql。

- **umadmin**

  用于首次登录到 Unified Manager。此用户被分配了 “应用程序管理员” 用户角色，并被配置为 “维护用户” 类型。此用户由 Unified Manager 创建。

- **jboss**

  用于运行与 JBoss 实用程序相关的 Unified Manager 服务。此用户由 Unified Manager 创建。

- **mysql**

  用于运行 Unified Manager 的 MySQL 数据库查询。此用户由 MySQL 第三方实用程序创建。

除了这些用户之外，Unified Manager 还会创建相应的组：maintenance、jboss 和 mysql。maintenance 和 jboss 组由 Unified Manager 创建，而 mysql 组由第三方实用程序创建。

如果在安装 Unified Manager 之前创建了自定义主目录并定义了自己的 umadmin 用户密码，则安装程序不会重新创建维护组或 umadmin 用户。

在 **Active IQ Unified Manager** 中更改 **JBoss** 密码

您可以重置在安装过程中设置的特定于实例的 JBoss 密码。如果您的站点需要此安全功能来覆盖 Unified Manager 安装设置，您可以选择重置密码。此操作还会更改 JBoss 用于访问 MySQL 的密码。

- 您必须具有对安装了 Unified Manager 的 Red Hat Enterprise Linux 系统的 root 用户访问权限。
- 您必须能够访问目录 `/opt/netapp/essentials/bin`中由 NetApp 提供的 `password.sh`脚本。

步骤

1. 以 root 用户登录系统。
2. 按所示顺序输入以下命令，停止 Unified Manager 服务：

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

   请勿停止关联的 MySQL 软件。

3. 输入以下命令以开始密码更改过程：

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

4. 出现提示时，请输入新的 JBoss 密码，然后再次输入以确认。

   请注意，密码应介于 8 到 16 个字符之间，必须至少包含一个数字、一个大写字母和一个小写字母，并且必须至少包含以下特殊字符之一：

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

5. 脚本完成后，按所示顺序输入以下命令，以启动 Unified Manager 服务：

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

6. 所有服务启动后，您可以登录到 Unified Manager UI。

在 **Red Hat Enterprise Linux** 上升级 **Unified Manager**

在 **Red Hat Enterprise Linux** 上升级 **Active IQ Unified Manager**

当新版本可用时，您可以升级 Unified Manager。

Unified Manager 软件的修补程序版本（如果由 NetApp 提供）使用与新版本相同的过程进行安装。

如果 Unified Manager 与 OnCommand Workflow Automation 实例配对，并且这两种产品都有可用的新版本软件，则必须断开这两种产品的连接，然后在执行升级后设置新的 Workflow Automation 连接。如果您仅对其中一款产品执行升级，则应在升级后登录 Workflow Automation，并验证其是否仍在从 Unified Manager 获取数据。

请对 **Active IQ Unified Manager** 版本使用受支持的升级路径

Active IQ Unified Manager 支持每个版本的特定升级路径。

并非所有版本的 Unified Manager 都可以就地升级到更高版本。Unified Manager 升级仅限于 N-2 模式。这意味着您只能在所有平台上升级到接下来的两个版本。例如，您只能从 Unified Manager 9.14 和 9.16 升级到 Unified Manager 9.18。

如果运行的版本早于受支持的版本，则需要先将 Unified Manager 实例升级到受支持的版本之一，然后再升级到当前版本。

例如，如果安装的版本是 Unified Manager 9.9，并且要升级到 Unified Manager 9.14，则需要执行一系列升级。

升级路径示例：

1. 升级 9.11 → 9.13
2. 升级 9.13 → 9.14
3. 升级 9.13 → 9.16
4. 升级 9.14 或 9.16 → 9.18

有关升级路径矩阵的更多信息，请参见此 "知识库（KB）文章"。

升级 **Active IQ Unified Manager**

您可以通过在 Linux 平台上下载并运行安装文件，从 Unified Manager 9.14 或 9.16 升级到 9.18。

开始之前

- 要升级 Unified Manager 的系统必须满足系统和软件要求。

  请参阅 "硬件系统要求"。

  请参阅 "Linux 软件和安装要求"。

- 您必须订阅 Red Hat Enterprise Linux 订阅管理器。
- 在升级 Unified Manager 之前，您必须安装或升级到正确版本的 OpenJDK。

  请参阅 "在 Linux 上升级 JRE"。

- 在升级 Unified Manager 之前，您必须安装或升级到正确版本的 7-zip。请参阅 "配置 7-zip 软件包"。
- 为避免数据丢失，您必须已创建 Unified Manager 数据库的备份，以防在升级过程中出现问题。NetApp 建议您将备份文件从 `/opt/netapp/data` 目录移动到外部位置。
- 在升级期间，系统可能会提示您确认是要将先前保留性能数据的默认设置保留 13 个月，还是将其更改为 6 个月。确认后，6 个月后将清除历史性能数据。

- 您应该已经完成了任何正在运行的操作，因为 Unified Manager 在升级过程中不可用。
- MySQL Community Edition 在 Unified Manager 升级期间自动升级。如果系统上安装的 MySQL 版本早于 8.4.10，则 Unified Manager 升级过程会自动将 MySQL 升级到 8.4.10。

步骤

1. 登录到目标 Red Hat Enterprise Linux 服务器。
2. 将 Unified Manager 捆绑包下载到服务器。

   请参阅 "下载 Linux 版 Unified Manager"。

3. 导航到目标目录并解压 Unified Manager 捆绑包：

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

   Unified Manager 所需的 RPM 模块已解压缩到目标目录。

4. 验证目录中是否存在以下模块：

   ```
   ls *.rpm
   ```

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

5. 运行预安装脚本，以确保没有可能与升级冲突的系统配置设置或任何已安装的软件：

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

   预安装脚本检查系统是否具有有效的 Red Hat Enterprise Linux 订阅，以及是否可以访问所需的软件存储库。如果脚本发现任何问题，您必须解决这些问题并继续升级。

   如果检测到任何缺失的软件包，请执行 "针对缺失的软件包要执行的其他步骤" 中所述的步骤。如果没有缺失的软件包，请继续执行后续步骤。

6. 使用以下脚本升级 Unified Manager：

   ```
   upgrade.sh
   ```

   此脚本自动执行 RPM 模块，升级必要的支持软件及其上运行的 Unified Manager 模块。此外，升级脚本会检查是否有任何系统配置设置或任何已安装的软件可能与升级冲突。如果脚本发现任何问题，则必须在升级 Unified Manager 之前解决这些问题。如果您在升级 Unified Manager 之前已安装包（如 *net-snmp*），MySQL 依赖项可能会在升级过程中卸载该包。您需要再次手动安装软件包才能继续使用。

7. 升级完成后，向后滚动浏览消息，直到看到显示 Unified Manager web UI 的 IP 地址或 URL、维护用户名（umadmin）和默认密码的消息。

   此消息与以下内容类似：

   ```
   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/
```

在受支持的 Web 浏览器的新窗口中输入指定的 IP 地址或 URL 以启动 Unified Manager Web UI，然后使用之前设置的相同维护用户名（umadmin）和密码登录。

针对缺失的软件包要执行的其他步骤

如果在升级期间您的站点检测到任何缺失的软件包，或者您的系统未连接到 Internet，或者您未使用 Red Hat Enterprise Linux 存储库，请执行以下步骤来确定您是否缺失任何所需的软件包并下载这些软件包。

这些步骤需要在主过程的步骤 *5* 之后执行。此过程将升级 Unified Manager，您无需执行任何其他升级步骤。

1. 查看可用和不可用的软件包列表：

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

   “Installing:”部分中的项目是当前目录中可用的包，而“Installing for dependencies:”部分中的项目是系统中缺少的包。

2. 在可以访问互联网的其他系统上，运行以下命令以下载丢失的程序包。

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

   这些软件包将下载到指定为 --downloaddir= 的目录中。

   由于插件 “yum-plugin-downloadonly” 在 Red Hat Enterprise Linux 系统上并不总是启用，因此您可能需要启用该功能以下载软件包而无需安装它：

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

3. 将下载的软件包复制到您在安装系统上解压缩 Unified Manager 捆绑包的目录。
4. 切换到该目录，然后运行以下命令以安装缺少的软件包及其依赖项。

   ```
   yum install *.rpm
   ```

5. 启动 Unified Manager 服务器。运行以下命令：

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

此过程完成 Unified Manager 升级过程。在受支持的 Web 浏览器的新窗口中输入指定的 IP 地址或 URL 以启动 Unified Manager Web UI，然后使用之前设置的相同维护用户名（umadmin）和密码登录。

升级 **Active IQ Unified Manager** 的 **Red Hat Enterprise Linux** 主机操作系统

如果您以前在 Red Hat Enterprise Linux 7.x 系统上安装了 Unified Manager，并且需要升

级到 Red Hat Enterprise Linux 8.x，则必须按照本主题中列出的过程之一进行操作。在这两种情况下，您都必须在 Red Hat Enterprise Linux 7.x 系统上创建 Unified Manager 备份，然后将备份还原到 Red Hat Enterprise Linux 8.x 系统上。请注意，支持的 Red Hat Enterprise Linux 版本为 8.0 到 8.10。

下面列出的两个选项之间的区别在于，在一种情况下，您在新的 8.x 服务器上执行 Unified Manager 恢复，而在另一种情况下，您在同一台服务器上执行恢复操作。

由于此任务要求您在 Red Hat Enterprise Linux 7.x 系统上创建 Unified Manager 备份，因此只有在准备好完成整个升级过程时才应创建备份，以便 Unified Manager 在最短时间内脱机。在 Red Hat Enterprise Linux 7.x 系统关闭期间以及新 Red Hat Enterprise Linux 8.x 启动之前，收集的数据中的间隙会显示在 Unified Manager UI 中。

如果您需要查看备份和还原过程的详细说明，请参见 "管理备份和还原操作"。

如果您有一个备用系统，可以在其上安装 Red Hat Enterprise Linux 8.x 软件，以便在 Red Hat Enterprise Linux 7.x 系统仍然可用的情况下在该系统上执行 Unified Manager 恢复，请执行以下步骤。

1. 使用 Red Hat Enterprise Linux 8.x 软件安装和配置新服务器。

   请参阅 "Linux 软件和安装要求"。

2. 在 Red Hat Enterprise Linux 8.x 系统上，安装与现有 Red Hat Enterprise Linux 7.x 系统上相同版本的 Unified Manager 软件。

   请参阅 "在 Linux 上安装 Unified Manager"。

   安装完成后，请勿启动 UI 或配置任何集群、用户或身份验证设置。在还原过程中，备份文件会填充此信息。

3. 在 Red Hat Enterprise Linux 7.x 系统上，从 Web UI 中的“管理”菜单创建 Unified Manager 备份，然后将备份文件 (`.7z` 文件）以及数据库存储库目录 (`/database-dumps-repo` 子目录）的内容复制到外部位置。
4. 在 Red Hat Enterprise Linux 7.x 系统上，关闭 Unified Manager。
5. 在 Red Hat Enterprise Linux 8.x 系统上，将备份文件 (`.7z` 文件）从外部位置复制到 `/opt/netapp/data/ocum-backup/`，并将数据库存储库文件复制到 `/ocum-backup` 目录下的 `/database-dumps-repo` 子目录。
6. 输入以下命令以从备份文件还原 Unified Manager 数据库：

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

7. 在 Web 浏览器中输入 IP 地址或 URL 以启动 Unified Manager Web UI，然后登录到系统。

验证系统正常运行后，您可以从 Red Hat Enterprise Linux 7.x 系统中删除 Unified Manager。

在同一台服务器上升级主机操作系统

如果没有可在其上安装 Red Hat Enterprise Linux 8.x 软件的备用系统，请执行以下步骤。

1. 从 Web UI 的“管理”菜单中，创建 Unified Manager 备份，然后将备份文件 (`.7z` 文件）和数据库存储库目录 (`/database-dumps-repo` 子目录）的内容复制到外部位置。

2. 从系统中删除 Red Hat Enterprise Linux 7.x 映像并完全擦除系统。
3. 在同一系统上安装和配置 Red Hat Enterprise Linux 8.x 软件。

   请参阅 "Linux 软件和安装要求"。

4. 在 Red Hat Enterprise Linux 8.x 系统上，安装与 Red Hat Enterprise Linux 7.x 系统上相同版本的 Unified Manager 软件。

   请参阅 "在 Linux 上安装 Unified Manager"。

   安装完成后，请勿启动 UI 或配置任何集群、用户或身份验证设置。在还原过程中，备份文件会填充此信息。

5. 将备份文件（(`.7z` 文件）从外部位置复制到 `/opt/netapp/data/ocum-backup/`，并将数据库存储库文件复制到 `/ocum-backup` 目录下的 `/database-dumps-repo` 子目录。
6. 输入以下命令以从备份文件还原 Unified Manager 数据库：

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

7. 在 Web 浏览器中输入 IP 地址或 URL 以启动 Unified Manager Web UI，然后登录到系统。

安装 Unified Manager 后升级第三方产品

安装 Active IQ Unified Manager 后升级第三方产品

如果已在 Linux 系统上安装了 Unified Manager，则可以升级第三方产品（例如 JRE）。

开发这些第三方产品的公司定期报告安全漏洞。您可以根据自己的时间表升级到此软件的更新版本。

升级 Linux 上的 OpenJDK for Active IQ Unified Manager

您可以在安装了 Unified Manager 的 Linux 服务器上升级到较新版本的 OpenJDK，以获取安全漏洞修复程序。

开始之前

您必须拥有安装了 Unified Manager 的 Linux 系统的 root 权限。

您可以在发行系列内更新 OpenJDK 发行版。例如，您可以从 OpenJDK 11.0.14 升级到 OpenJDK 11.0.17，但不能直接从 OpenJDK 11 更新到 OpenJDK 12。

步骤

1. 以 root 用户身份登录到 Unified Manager 主机。
2. 将相应版本的 OpenJDK（64 位）下载到目标系统。
3. 停止 Unified Manager 服务：

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

4. 在系统上安装最新的 OpenJDK。
5. 启动 Unified Manager 服务：

```
systemctl start ocie

systemctl start ocieau
```

重新启动 **Active IQ Unified Manager**

执行配置更改后，可能需要重新启动 Unified Manager。

开始之前

您必须具有对安装了 Unified Manager 的 Red Hat Enterprise Linux 服务器的 root 用户访问权限。

步骤

1. 以 root 用户身份登录到要重新启动 Unified Manager 服务的服务器。
2. 按以下顺序停止 Unified Manager 服务和关联的 MySQL 服务：

```
systemctl stop ocieau

systemctl stop ocie

systemctl stop mysqld
```

3. 按以下顺序启动 MySQL 和 Unified Manager 服务：

```
systemctl start mysqld

systemctl start ocie

systemctl start ocieau
```

`mysqld` 是启动和停止 MySQL 服务器所需的守护程序。

删除 **Active IQ Unified Manager**

可以使用单个命令从 Red Hat Enterprise Linux 主机停止和卸载 Unified Manager。

开始之前

- 您必须具有要从中删除 Unified Manager 的服务器的 root 用户访问权限。
- 必须在 Linux 系统上禁用安全增强型 Linux (SELinux)。使用 `setenforce 0` 命令将 SELinux 运行时模式更改为“`Permissive`”。
- 在删除软件之前，必须从 Unified Manager 服务器中删除所有集群（数据源）。
- 您应该手动删除为允许或阻止 MySQL 端口 3306 而创建的防火墙规则。防火墙规则不会自动删除。

步骤

1. 以 root 用户身份登录到要删除 Unified Manager 的服务器。
2. 停止并从服务器中删除 Unified Manager：

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

   此步骤删除所有关联的 NetApp RPM 包。它不删除必备软件模块，例如 Java、MySQL 和 7zip。

3. *可选：*如果适用，请删除支持的软件模块，例如 Java、MySQL 和 7zip：

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

此操作完成后，将删除软件。卸载后， `/opt/netapp/data`目录中的所有数据都会移动到 `/opt/netapp/data/BACKUP`文件夹中。卸载 Unified Manager 也会删除 Java 和 MySQL 软件包，除非系统上的任何其他应用程序需要并使用这些软件包。但是，MySQL 数据不会被删除。

删除 **Active IQ Unified Manager** 的自定义 **umadmin** 用户和 **maintenance** 组

如果在安装 Unified Manager 之前创建了自定义主目录以定义自己的 umadmin 用户和维护帐户，则应在卸载 Unified Manager 后删除这些项目。

标准的 Unified Manager 卸载不会删除自定义的 umadmin 用户和维护帐户。您必须手动删除这些项目。

步骤

1. 以 root 用户身份登录到 Red Hat Enterprise Linux 服务器。
2. 删除 umadmin 用户：

   ```
   userdel umadmin
   ```

3. 删除维护组：

   ```
   groupdel maintenance
   ```

在 Windows 系统上安装 Unified Manager

Active IQ Unified Manager 简介

了解Active IQ Unified Manager

Active IQ Unified Manager（以前称为 OnCommand Unified Manager）使您能够从单个界面监控和管理 ONTAP 存储系统的运行状况和性能。您可以在 Linux 服务器、Windows 服务器或 VMware 主机上作为虚拟应用装置部署 Unified Manager。

完成安装并添加要管理的集群后，Unified Manager 将提供显示受监视存储系统的容量、可用性、保护和性能状态的图形界面。

相关信息

"NetApp 互操作性表工具"

了解 Active IQ Unified Manager 服务器的作用

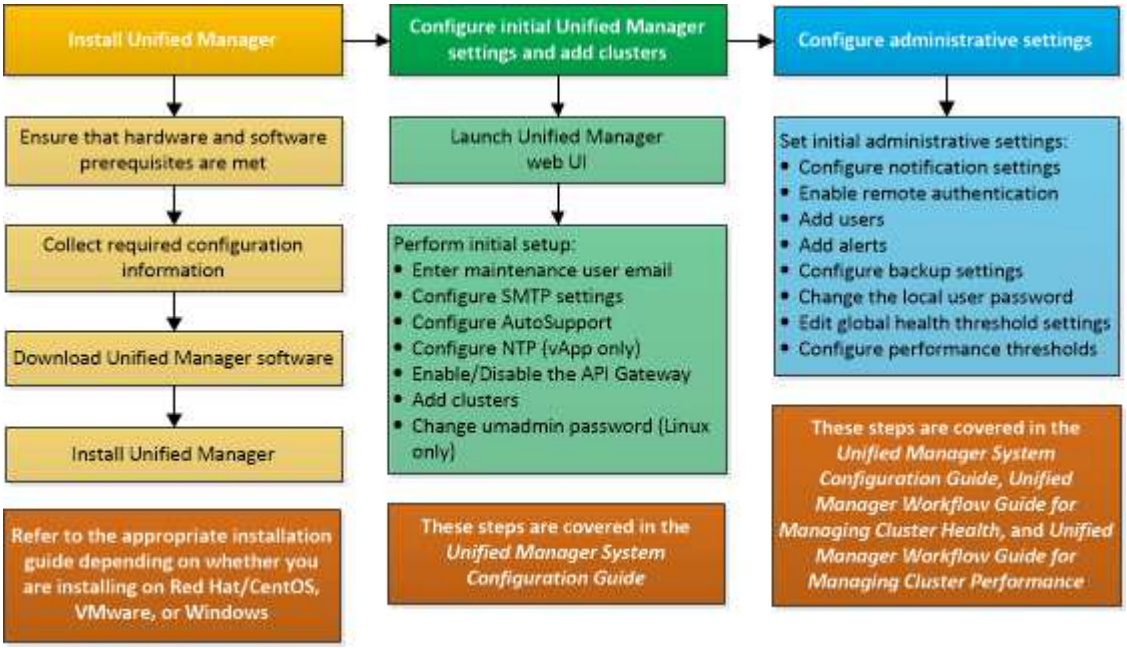
Unified Manager 服务器基础架构由数据收集单元、数据库和应用程序服务器组成。它提供基础架构服务，例如发现、监视、基于角色的访问控制（RBAC）、审核和记录。

Unified Manager 收集群集信息，将数据存储在数据库中，并分析数据以查看是否存在任何群集问题。

了解 Active IQ Unified Manager 的安装顺序

安装工作流描述了在使用 Unified Manager 之前必须执行的任务。

这些部分介绍了以下工作流程中显示的每个项目。



安装 Unified Manager 的要求

确保服务器满足 Active IQ Unified Manager 安装要求

在开始安装过程之前，请确保要安装 Unified Manager 的服务器满足特定的软件、硬件、CPU 和内存要求。

NetApp 不支持对 Unified Manager 应用程序代码进行任何修改。如果需要对 Unified Manager 服务器应用任何安全措施，则应对安装 Unified Manager 的操作系统进行这些更改。

有关将安全措施应用于 Unified Manager 服务器的详细信息，请参见知识库文章。

"应用于 Active IQ Unified Manager for Clustered Data ONTAP 的安全措施的可支持性"

相关信息

"NetApp 互操作性表工具"

了解 Active IQ Unified Manager 的虚拟基础架构和硬件要求

在虚拟基础架构或物理系统上安装 Unified Manager 应满足内存、CPU 和磁盘空间的最低要求。

下表显示了建议的内存、CPU 和磁盘空间资源值。这些值已经过验证，以确保 Unified Manager 达到可接受的性能水平。

硬件配置	建议的设置
RAM	12 GB
处理器	4 个 CPU
CPU 周期容量	总共 9572 MHz（最低要求 9572 MHz）
可用磁盘空间	150 GB，其中容量分配如下： • 安装目录的 100 GB 磁盘空间 • 用于 MySQL 数据目录的 50 GB 磁盘空间

Unified Manager 可以安装在内存较小的系统上，但建议使用 12 GB RAM，以确保有足够的内存来实现最佳性能，并使系统能够在配置增长时容纳更多的集群和存储对象。您不应在部署 Unified Manager 的虚拟机上设置任何内存限制，也不应启用任何阻碍软件利用系统上分配的内存的功能（例如内存气球机制）。

此外，在安装 Unified Manager 的第二个实例之前，Unified Manager 的单个实例可以监视的节点数是有限制的。有关节点限制、CPU 和内存建议，请参阅 "Unified Manager 最佳实践指南"。

内存页面交换会对系统和管理应用程序的性能产生负面影响。竞争由于整体主机利用率而无法使用的 CPU 资源可能会降低性能。

专用要求

安装 Unified Manager 的物理或虚拟系统应专门用于 Unified Manager，不应与其他应用程序共享。其他应用程序可能会消耗系统资源，并可能大幅降低 Unified Manager 的性能。

备份的空间要求

如果您计划使用 Unified Manager 备份和还原功能，请分配额外的容量，以便“`data`”目录或磁盘具有 150 GB 的空间。备份可以写入本地目标或远程目标。最佳做法是确定 Unified Manager 主机系统外部具有至少 150 GB 空间的远程位置。

主机连接要求

安装 Unified Manager 的物理系统或虚拟系统应进行相应配置，以便您可以从主机本身成功 `ping`主机名。如果是 IPv6 配置，您应验证对主机名的 `ping6`是否成功，以确保 Unified Manager 安装成功。

您可以使用主机名（或主机 IP 地址）访问产品 Web UI。如果在部署期间为网络配置了静态 IP 地址，则您已为网络主机指定了名称。如果使用 DHCP 配置了网络，则应从 DNS 获取主机名。

如果您计划允许用户使用短名称而不是使用完全限定的域名（FQDN）或 IP 地址来访问 Unified Manager，则您的网络配置必须将此短名称解析为有效的 FQDN。

了解 **Active IQ Unified Manager** 的 **Windows** 软件和安装要求

若要在 Windows 上成功安装 Unified Manager，应确保安装 Unified Manager 的系统满足软件要求。

操作系统软件

可以在以下 Windows 版本上安装 Unified Manager：

- Microsoft Windows Server 2019 标准版和数据中心版
- Microsoft Windows Server 2022 标准版和数据中心版

Unified Manager 在 64 位 Windows 操作系统上支持以下语言：

- 英语
- 日语
- 简体中文

有关受支持的 Windows 版本的完整和最新列表，请参见互操作性矩阵。

"mysupport.netapp.com/cn/matrix"

NetApp 不支持使用第三方工具（例如 Microsoft System Center Configuration Manager (SCCM)）安装 Unified Manager。

服务器应专用于运行 Unified Manager。不应在服务器上安装其他应用程序。由于公司规定，您的 Windows 系统上可能安装了处于活动状态的防病毒软件。您应在安装 Unified Manager 之前禁用防病毒软件，以防止安装失败。

第三方软件

以下第三方软件包与 Unified Manager 捆绑在一起。如果这些第三方软件包未安装在您的系统上，则 Unified Manager 会将它们作为安装的一部分进行安装。

- 适用于 Visual Studio 2015 的 Microsoft Visual C++ 可再发行组件包版本 14.29.30133.0
- MySQL Community Edition 8.4.10 版
- Python 3.13.3
- OpenJDK 版本 17.0.15+6
- 7-zip 版本 25.01 或更高版本

从 Unified Manager 9.5 开始，OpenJDK 在 Unified Manager 安装包中提供并自动安装。从 Unified Manager 9.5 开始，不支持 Oracle Java。

如果 MySQL 已预安装，您应确保：

- 它正在使用默认端口。
- 未安装示例数据库。
- 服务名称为“`MYSQL84`”。

Unified Manager 部署在 WildFly Web 服务器上。WildFly 27.0.1.Final 与 Unified Manager 捆绑并配置。

在升级任何第三方软件之前，应关闭正在运行的 Unified Manager 实例。第三方软件安装完成后，您可以重新启动 Unified Manager。

安装要求

- 应安装 Microsoft .NET 4.5.2 或更高版本。
- 该 `temp`目录应配置 `2 GB` 的磁盘空间用于提取安装文件。要验证目录是否已创建，请在命令行界面上运行以下命令： `echo %temp%`
- 您应该在 Windows 驱动器中保留 2 GB 的磁盘空间来缓存 Unified Manager MSI 文件。
- 要安装 Unified Manager 的 Microsoft Windows Server 应配置完全限定域名（FQDN），以便 `ping`对主机名和 FQDN 的响应成功。
- 您应禁用 Microsoft IIS 万维网发布服务，并确保端口 80 和 443 空闲。
- 应确保在安装过程中禁用“`Windows Installer RDS Compatibility`”的远程桌面会话主机设置。
- UDP 端口 514 应该是空闲的，不应被任何其他服务使用。
- 在安装 Unified Manager 之前，应禁用系统上的所有防病毒软件。安装完成后，请确保从防病毒扫描中手动排除以下路径：
  - Unified Manager 数据目录，例如， `C:\ProgramData\NetApp\OnCommandAppData\`
  - Unified Manager 安装目录，例如， `\C:\Program Files\NetApp\`
  - MySQL 数据目录，例如， `C:\ProgramData\MySQL\MySQLServerData`

在 **Active IQ Unified Manager** 中使用受支持的浏览器

要访问 Unified Manager Web UI，请使用受支持的浏览器。

互操作性矩阵包含支持的浏览器版本列表。

"mysupport.netapp.com/cn/matrix"

对于所有浏览器，禁用弹出窗口拦截器可确保正确显示软件功能。

如果您计划为 SAML 身份验证配置 Unified Manager，以便身份提供程序（IdP）可以对用户进行身份验证，则还应检查 IdP 支持的浏览器列表。

了解 **Active IQ Unified Manager** 的协议和端口要求

所需的端口和协议支持 Unified Manager 服务器与托管存储系统、服务器和其他组件之间的通信。

到 **Unified Manager** 服务器的连接

在典型安装中，连接到 Unified Manager Web UI 时不必指定端口号，因为始终使用默认端口。例如，由于 Unified Manager 始终尝试在其默认端口上运行，因此您可以输入 `https://<host>`而不是 `https://<host>:443`。

Unified Manager 服务器使用特定协议访问以下接口：

接口	协议	端口	问题描述
Unified Manager Web UI	HTTP	80	用于访问 Unified Manager Web UI；自动重定向到安全端口 443。
Unified Manager Web UI 和使用 API 的程序	HTTPS	443	用于安全地访问 Unified Manager Web UI 或进行 API 调用；只能使用 HTTPS 进行 API 调用。
维护控制台	SSH/SFTP	22	用于访问维护控制台并检索支持包。
Linux 命令行	SSH/SFTP	22	用于访问 Red Hat Enterprise Linux 命令行并检索支持捆绑包。
系统日志	UDP	514	用于从 ONTAP 系统访问基于订阅的 EMS 消息，并根据这些消息创建事件。
REST	HTTPS	9443	用于从经过身份验证的 ONTAP 系统访问基于实时 REST API 的 EMS 事件。

接口	协议	端口	问题描述
MySQL 数据库	MySQL	3306	用于启用 OnCommand Workflow Automation 和 OnCommand API Services 对 Unified Manager 的访问。
AMQP QPID 代理	TCP/IP	56072	用于内部消息通信。
AMQP QPID 代理	WebSocket over TCP	56080	用于在此端口上侦听从 ONTAP（云代理）接收的消息。
AMQP QPID 代理	WebSocket over TCP	56443	用于在此端口上侦听从 ONTAP（云代理）接收的消息。此端口上的通信支持 TLS 或 SSL 提供的加密。

在 Windows 系统上安装 Unified Manager 时，MySQL 的默认端口 3306 仅限于本地主机。安装完成后，启用防火墙以限制对 MySQL 端口 3306 的访问。这不会影响任何保留先前配置的升级场景。此配置可以修改，并且可以通过使用维护控制台上的 `Control access to MySQL port 3306`选项使连接可供其他主机使用。有关信息，请参见"其他菜单选项"。可以使用 Unified Manager 维护控制台更改用于 HTTP 和 HTTPS 通信的端口（端口 80 和 443）。有关详细信息，请参见"配置 Active IQ Unified Manager"。

来自 **Unified Manager** 服务器的连接

您应将防火墙配置为打开端口，以启用 Unified Manager 服务器与受管存储系统、服务器和其他组件之间的通信。如果端口未打开，则通信失败。

根据您的环境，可以选择修改 Unified Manager 服务器用于连接到特定目标的端口和协议。

Unified Manager 服务器使用以下协议和端口连接到托管存储系统、服务器和其他组件：

目标	协议	端口	问题描述
存储系统	HTTPS	443/TCP	用于监控和管理存储系统。
存储系统	NDMP	10000/TCP	用于某些 Snapshot 还原操作。
AutoSupport 服务器	HTTPS	443	用于发送 AutoSupport 信息。需要互联网访问才能执行此功能。
身份验证服务器	LDAP	389	用于发出身份验证请求以及用户和组查找请求。
LDAPS	636	用于安全 LDAP 通信。	邮件服务器
SMTP	25	用于发送警报通知电子邮件。	SNMP 陷阱发送方

目标	协议	端口	问题描述
SNMPv1 或 SNMPv3	162/UDP	用于发送警报通知 SNMP 陷阱。	外部数据提供程序服务器
TCP	2003	用于将性能数据发送到外部数据提供程序，例如 Graphite。	NTP 服务器
NTP	123/UDP	用于将 Unified Manager 服务器上的时间与外部 NTP 时间服务器同步。（仅限 VMware 系统）	AMQP QPID 代理
TCP/IP	56072	用于内部消息通信。	AMQP QPID 代理
WebSocket over TCP	56080	用于在此端口上侦听从 ONTAP（云代理）接收的消息。	AMQP QPID 代理
WebSocket over TCP	56443	用于在此端口上侦听从 ONTAP（云代理）接收的消息。通过此端口进行的通信支持 TLS 或 SSL 提供的加密。	系统日志

在 **Active IQ Unified Manager** 中填写工作表

在安装和配置 Unified Manager 之前，应准备好有关环境的特定信息。您可以在工作表中记录信息。

Unified Manager 安装信息

安装 Unified Manager 所需的详细信息。

部署软件的系统	您的价值
主机完全限定的域名	
主机 IP 地址	
网络掩码	
网关 IP 地址	
主 DNS 地址	
辅助 DNS 地址	
搜索域	
维护用户名	
维护用户密码	

Unified Manager 配置信息

安装后配置 Unified Manager 的详细信息。某些值是可选的，具体取决于您的配置。

设置	您的价值
维护用户电子邮件地址	
SMTP 服务器主机名或 IP 地址	
SMTP 用户名	
SMTP 密码	
SMTP 端口	25（默认值）
发送警报通知的电子邮件	
身份验证服务器主机名或 IP 地址	
Active Directory 管理员名称或 LDAP 绑定可分辨名称	
Active Directory 密码或 LDAP 绑定密码	
身份验证服务器基本可分辨名称	
身份提供程序（IdP）URL	
身份提供程序（IdP）元数据	
SNMP 陷阱目标主机 IP 地址	
SNMP 端口	

集群信息

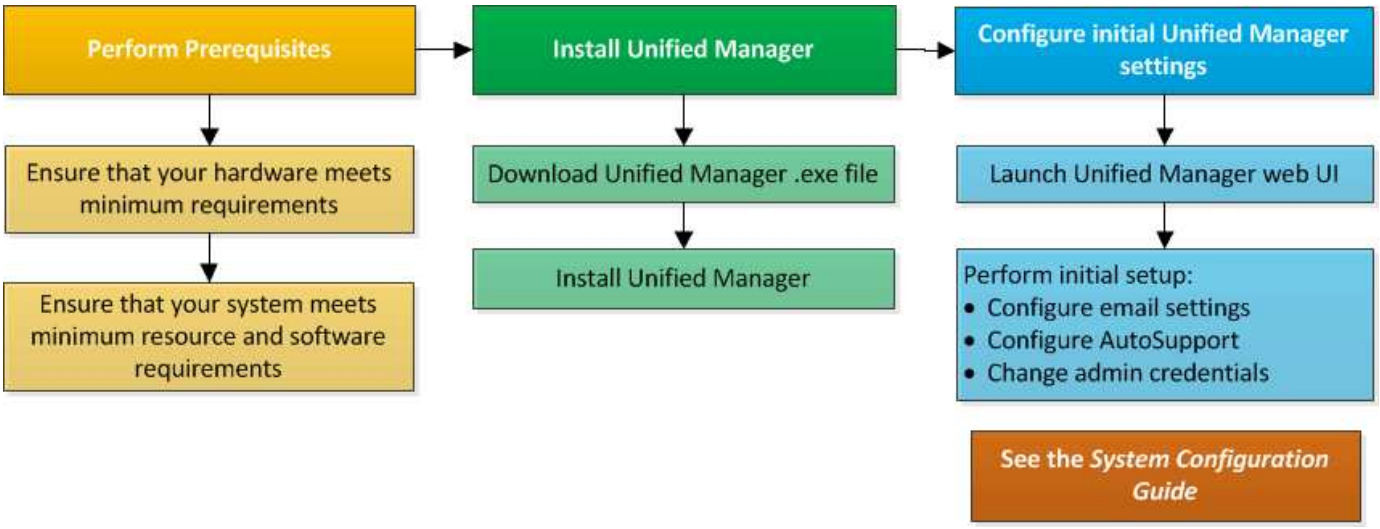
使用 Unified Manager 管理的存储系统的详细信息。

第 **1** 个集群，共 **N** 个	您的价值
主机名或集群管理 IP 地址	
ONTAP 管理员用户名 必须为管理员分配“admin”角色。	
ONTAP 管理员密码	
协议	HTTPS

安装、升级和删除 **Unified Manager** 软件

了解在 **Windows** 上安装 **Active IQ Unified Manager** 的过程

安装工作流描述了在使用 Unified Manager 之前必须执行的任务。



在 Windows 上安装 Unified Manager

在 Windows 上安装 Active IQ Unified Manager

您可以安装 Unified Manager 来监控和排除数据存储容量、可用性、性能和保护问题。

开始之前

- 您计划安装 Unified Manager 的系统应满足系统和软件要求。

  请参阅 "硬件系统要求"。

  请参阅 "Windows 软件和安装要求"。

  > 从 Unified Manager 9.5 开始，安装包中提供了 OpenJDK 并会自动安装。从 Unified Manager 9.5 开始，不再支持 Oracle Java。

- 您应具有 Windows 管理员权限。请确保您的用户名不以感叹号“!`". Installation of Unified Manager might fail if the user name of user running the installation begins with "!`”开头。
- 支持所有集群，但 ASA r2 系统除外。
- 您应具有受支持的 Web 浏览器。
- Unified Manager 维护用户密码应介于 8 到 20 个字符之间，应包含大写字母或小写字母、数字和特殊字符。
- 维护用户或 MySQL root 用户的密码字符串中不允许使用以下特殊字符：" ' ` % , = & < > | ^ \ / ( ) [ ] ;:

  允许使用以下特殊字符：~ ! @ # $ * - ? .+ { }

步骤

1. 使用默认本地管理员帐户登录到 Windows。
2. 登录到 NetApp 支持站点，然后导航到 Unified Manager 的下载页面：

   "NetApp 支持站点"

3. 选择所需的 Unified Manager 版本并接受最终用户许可协议（EULA）。
4. 将 Unified Manager Windows 安装文件或 zip 文件下载到 Windows 系统上的目标目录。
5. 如果需要，请提取 zip 文件，然后导航到安装文件所在的目录。
6. 右键单击并以管理员身份运行 Unified Manager 安装程序可执行文件（.exe）。

   Unified Manager 检测缺失或预安装的第三方软件包并将其列出。如果系统中未安装所需的第三方软件包，Unified Manager 会在安装过程中将其安装。

7. 单击*下一步*。
8. 输入用户名和密码以创建维护用户。
9. 在数据库连接向导中，输入 MySQL root 密码。
10. 单击*更改*以指定 Unified Manager 安装目录和 MySQL 数据目录的新位置。

    如果不更改安装目录，则将在默认安装目录中安装 Unified Manager。

11. 单击*下一步*。
12. 在 Ready to Install Shield 向导中，单击 **Install**。
13. 安装完成后，单击 **Finish**。
14. 如果您的 Windows 系统上安装了活动的防病毒软件，请在安装完成后从防病毒扫描中手动排除以下路径：
    - Unified Manager 数据目录
    - Unified Manager 安装目录
    - MySQL 数据目录

安装将创建多个目录：

- 安装目录

  这是在安装过程中指定的 Unified Manager 的根目录。示例： `C:\Program Files\NetApp\`

- MySQL 数据目录

  这是存储 MySQL 数据库的目录，您在安装过程中指定了此目录。示例：
  `C:\ProgramData\MySQL\MySQLServerData\`

- Java 目录

  这是安装 OpenJDK 的目录。示例： `C:\Program Files\NetApp\JDK\`

- Unified Manager 应用程序数据目录（appDataDir）

  这是存储所有应用程序生成的数据的目录。这包括日志、支持捆绑包、备份和所有其他附加数据。示例：
  `C:\ProgramData\NetApp\OnCommandAppData\`

您可以访问 Web UI 以执行 Unified Manager 的初始设置，如 "配置 Active IQ Unified Manager" 中所述。

执行 **Active IQ Unified Manager** 的无人值守安装

您可以使用命令行界面安装 Unified Manager，而无需用户干预。您可以通过以键值对形式传递参数来完成无人参与安装。

步骤

1. 使用默认的本地管理员帐户登录到 Windows 命令行界面。
2. 导航到要安装 Unified Manager 的位置，然后选择以下选项之一：

选项	**AutoSupport**

如果预安装了第三方软件包	`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"`
	
	示例：
	
	`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"`

如果未安装第三方软件包	`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"`
	
	示例：
	
	`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"`

该 `/qr` 选项可启用精简用户界面的静默模式。此时将显示一个基本的用户界面，其中显示安装进度。系统不

会提示您进行输入。如果未预安装 JRE、MySQL 和 7zip 等第三方软件包，则应使用 `/qr` 选项。如果在未安装第三方软件包的服务器上使用 `/qn` 选项，则安装将失败。

该 `/qn`选项启用无用户界面的静默模式。在安装过程中不会显示任何用户界面或详细信息。未安装第三方软件包时，不应使用 `/qn`选项。

3. 使用以下 URL 登录到 Unified Manager Web 用户界面：

   `https://IP address`

在 **Active IQ Unified Manager** 中更改 **Windows** 上的 **JBoss** 密码

您可以重置在安装过程中设置的特定于实例的 JBoss 密码。如果您的站点需要此安全功能来覆盖 Unified Manager 安装设置，您可以选择重置密码。此操作还会更改 JBoss 用于访问 MySQL 的密码。

开始之前

- 您应具有安装 Unified Manager 的系统的 Windows 管理员权限。
- 您应该拥有 MySQL root 用户的密码。
- 您应该能够访问目录中由 NetApp 提供的 `password.bat`脚本

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

步骤

1. 以 admin 用户身份登录到 Unified Manager 主机。
2. 使用 Windows 服务控制台停止以下 Unified Manager 服务：
   - NetApp Active IQ 采集服务（Ocie-au）
   - NetApp Active IQ 管理服务器服务（Oncommandsvc）
3. 启动 `password.bat` 脚本以开始密码更改过程：

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

4. 出现提示时，输入 MySQL root 用户密码。
5. 出现提示时，请输入新的 JBoss 用户密码，然后再次输入以确认。

   请注意，密码应介于 8 到 16 个字符之间，必须至少包含一个数字、一个大写字母和一个小写字母，并且必须至少包含以下特殊字符之一：

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

6. 脚本完成后，使用 Windows 服务控制台启动 Unified Manager 服务：
   - NetApp Active IQ 管理服务器服务（Oncommandsvc）
   - NetApp Active IQ 采集服务（Ocie-au）
7. 所有服务启动后，您可以登录到 Unified Manager UI。

请对 **Active IQ Unified Manager** 版本使用受支持的升级路径

Active IQ Unified Manager 支持每个版本的特定升级路径。

并非所有版本的 Unified Manager 都可以就地升级到更高版本。Unified Manager 升级仅限于 N-2 模式。这意味着您只能在所有平台上升级到接下来的两个版本。例如，您只能从 Unified Manager 9.14 和 9.16 升级到 Unified Manager 9.18。

如果运行的版本早于受支持的版本，则需要先将 Unified Manager 实例升级到受支持的版本之一，然后再升级到当前版本。

例如，如果安装的版本是 Unified Manager 9.9，并且要升级到 Unified Manager 9.14，则需要执行一系列升级。

升级路径示例：

1. 升级 9.11 → 9.13
2. 升级 9.13 → 9.14
3. 升级 9.13 → 9.16
4. 升级 9.14 或 9.16 → 9.18

有关升级路径矩阵的更多信息，请参见此 "知识库（KB）文章"。

在 **Windows** 上升级 **Active IQ Unified Manager**

您可以通过在 Windows 平台上下载并运行安装文件，将 Unified Manager 9.14 或 9.16 升级到 9.18。

开始之前

- 您要升级 Unified Manager 的系统应满足系统和软件要求。

  请参阅 "硬件系统要求"。

  请参阅 "Windows 软件和安装要求"。

  > 从 Unified Manager 9.5 开始，安装包中提供了 OpenJDK 并会自动安装。从 Unified Manager 9.5 开始，不再支持 Oracle Java。

  > 开始升级之前，请确保系统上已安装 Microsoft .NET 4.5.2 或更高版本。

- MySQL Community Edition 在 Unified Manager 升级期间自动升级。如果系统上安装的 MySQL 版本早于 8.4.10，则 Unified Manager 升级过程会自动将 MySQL 升级到 8.4.10。您不得对早期版本的 MySQL 单独执行升级至 8.4.10 的操作。
- 除 ASA r2 系统外，支持所有集群。
- 您应具有 Windows 管理员权限。请确保您的用户名不以感叹号“!`". Installation of Unified Manager might fail if the user name of user running the installation begins with "!`”开头。
- 您应具有有效的凭据才能登录到 NetApp 支持站点。

- 为了避免数据丢失，您应该已经创建了 Unified Manager 计算机的备份，以防在升级期间出现问题。
- 您应该有足够的磁盘空间来执行升级。

  安装驱动器上的可用空间应比数据目录的大小大 2.5 GB。如果可用空间不足，升级将停止并显示一条错误消息，指示要添加的空间量。

- 在升级期间，系统可能会提示您确认是要保留先前将性能数据保留 13 个月的默认设置，还是将其更改为 6 个月。确认后，超过 6 个月的历史性能数据将被清除。
- 在升级之前，应关闭_<InstallDir>\JDK_和_MySQL 数据目录_中任何打开的文件或文件夹。
- 如果您的 Windows 系统上安装了活动的防病毒软件，则 Unified Manager 升级可能会失败。在升级 Unified Manager 之前，应禁用系统中的所有病毒扫描软件。

在升级过程中，Unified Manager 不可用。在升级 Unified Manager 之前，您应完成所有正在运行的操作。

如果 Unified Manager 与 OnCommand Workflow Automation 实例配对，并且这两种产品都有可用的新版本软件，则必须断开这两种产品的连接，然后在执行升级后设置新的 Workflow Automation 连接。如果您仅对其中一款产品执行升级，则应在升级后登录 Workflow Automation，并验证其是否仍在从 Unified Manager 获取数据。

步骤

1. 登录到 NetApp 支持站点，然后导航到 Unified Manager 的下载页面：

   "NetApp 支持站点"。

2. 选择所需的 Unified Manager 版本并接受最终用户许可协议（EULA）。
3. 将 Unified Manager Windows 安装文件或 zip 文件下载到 Windows 系统上的目标目录。如果需要，请提取 zip 文件，然后导航到安装文件所在的目录。右键单击并以管理员身份运行 Unified Manager 安装程序可执行文件（.exe）。

   Unified Manager 将提示您以下消息：

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

4. 单击*是*，然后单击*下一步*。
5. 输入安装过程中设置的 MySQL84 root 密码，然后单击 下一步。
6. 在受支持的 Web 浏览器上的新窗口中启动 Web UI，然后登录以使用升级版本的 Unified Manager。
7. 如果您的 Windows 系统上安装了处于活动状态的防病毒软件，请确保在升级完成后从防病毒扫描中手动排除以下路径：
   - Unified Manager 数据目录
   - Unified Manager 安装目录
   - MySQL 数据目录

要执行 Unified Manager 的静默升级，请运行以下命令：
`ActiveIQUnifiedManager-<version\>.exe /s /v"MYSQL_PASSWORD=<password> /qn /l*v <system_drive>:\install.log"`

升级第三方产品

在 **Windows** 上的 **Active IQ Unified Manager** 中升级第三方产品

安装在 Windows 系统上时，可以在 Unified Manager 上升级第三方产品（例如 JRE）。

开发这些第三方产品的公司定期报告安全漏洞。您可以根据自己的时间表升级到此软件的更新版本。

升级 **Windows** 上的 **Active IQ Unified Manager** 的 **OpenJDK**

您可以在安装了 Unified Manager 的 Windows 服务器上升级到较新版本的 OpenJDK，以获取安全漏洞修复程序。

开始之前

您必须具有安装 Unified Manager 的系统的 Windows 管理员权限。

您可以在发行系列内更新 OpenJDK 发行版。例如，您可以从 OpenJDK 11.0.16 升级到 OpenJDK 11.0.18，但不能直接从 OpenJDK 11 更新到 OpenJDK 12。

步骤

1. 以 admin 用户身份登录到 Unified Manager 主机。
2. 将相应版本的 OpenJDK（64 位）从 OpenJDK 站点下载到目标系统。

   例如，从 "Oracle Java SE 17 存档下载页面" 下载 `jdk-17.0.15_windows-x64_bin.zip` 文件。

   > 需要 Oracle 帐户才能下载该文件。如果您没有 Oracle 帐户，请转到 "Oracle 帐户登录页面" 创建一个。

3. 使用 Windows 服务控制台停止以下 Unified Manager 服务：
   - NetApp Active IQ 采集服务（Ocie-au）
   - NetApp Active IQ 管理服务器服务（Oncommandsvc）
4. 展开 `zip`文件。
5. 将目录和文件从生成的 `jdk`目录（例如， `jdk-11.0.18`复制到安装 `Java` 的位置。示例：`C:\Program Files\NetApp\JDK\`
6. 使用 Windows 服务控制台启动 Unified Manager 服务：
   - NetApp Active IQ 管理服务器服务（Oncommandsvc）
   - NetApp Active IQ 采集服务（Ocie-au）

卸载 **Active IQ Unified Manager** 中的第三方产品

升级 Unified Manager 后，您可以卸载第三方产品，如 Python 或 Microsoft Visual C++ 2013。这是可选的。

卸载 **Python**

步骤

1. 从*控制面板*中选择*程序* > 程序和功能。
2. 从程序列表中选择 Python。
3. 选择*卸载此程序*。卸载除 3.13.3 之外的任何版本的 Python。确保保留 Python 版本 3.13.3。

卸载 **Microsoft Visual C++ 2013**

步骤

1. 从*控制面板*中选择*程序* > 程序和功能。
2. 从程序列表中选择 **Microsoft Visual C++ 2013**。
3. 选择*卸载此程序*。

在 **Windows** 上重新启动 **Active IQ Unified Manager**

执行配置更改后，可能需要重新启动 Unified Manager。

开始之前

您必须具有 Windows 管理员权限。

步骤

1. 使用默认本地管理员帐户登录到 Windows。
2. 停止 Unified Manager 服务：

从……	按以下顺序停止服务……
命令行	a. `sc stop ocie-au` b. `sc stop Oncommandsvc`
Microsoft Service Manager	a. NetApp Active IQ 采集服务（Ocie-au） b. NetApp Active IQ 管理服务器服务（Oncommandsvc）

3. 启动 Unified Manager 服务：

从……	按以下顺序启动服务……
命令行	a. `sc start Oncommandsvc` b. `sc start ocie-au`
Microsoft Service Manager	a. NetApp Active IQ 管理服务器服务（Oncommandsvc） b. NetApp Active IQ 采集服务（Ocie-au）

卸载 **Active IQ Unified Manager**

您可以通过使用程序和功能向导或从命令行界面执行无人参与卸载来卸载 Unified Manager。

开始之前

- 您必须具有 Windows 管理员权限。
- 在卸载软件之前，必须从 Unified Manager 服务器中删除所有集群（数据源）。
- 您应该手动删除为允许或阻止 MySQL 端口 3306 而创建的防火墙规则。防火墙规则不会自动删除。

步骤

1. 通过选择以下选项之一卸载 Unified Manager：
   - 如果从*程序和功能*向导中卸载 Unified Manager，请执行以下步骤：
     i. 导航到*控制面板* > 程序和功能。
     ii. 选择 Active IQ Unified Manager，然后单击*卸载*。
   - 如果从命令行卸载 Unified Manager，请执行以下步骤：
     i. 使用管理员权限登录到 Windows 命令行。
     ii. 请导航到 Active IQ Unified Manager 目录，然后运行以下命令：

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

     如果已在服务器上启用用户帐户控制（UAC），并且以域用户身份登录，则必须使用命令行卸载方法。

   已从系统中卸载 Unified Manager。
2. 卸载在 Unified Manager 卸载过程中未删除的以下第三方软件包和数据：
   - 第三方软件包：JRE、MySQL、Microsoft Visual C++ 2015 Redistributable、Python 和 7zip
   - Unified Manager 生成的 MySQL 应用程序数据
   - 应用程序日志和应用程序数据目录的内容

执行配置和管理任务

配置 Active IQ Unified Manager

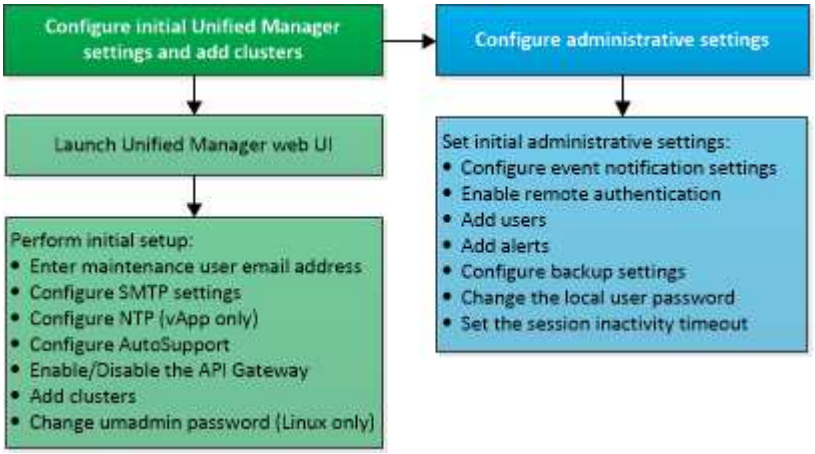
了解有关配置 Active IQ Unified Manager 的信息

安装 Active IQ Unified Manager（以前称为 OnCommand Unified Manager）后，必须完成初始设置（也称为首次体验向导）才能访问 Web UI。然后，您可以执行其他配置任务，例如添加集群、配置远程身份验证、添加用户和添加警报。

完成 Unified Manager 实例的初始设置需要执行本手册中描述的部分步骤。其他步骤是推荐的配置设置，这些设置有助于在新实例上进行设置，或者在开始定期监控 ONTAP 系统之前最好能有所了解。

了解 Active IQ Unified Manager 中的配置顺序

配置工作流描述了在使用 Unified Manager 之前必须执行的任务。



访问 Active IQ Unified Manager 中的 Web UI

安装 Unified Manager 后，您可以访问 Web UI 以设置 Unified Manager，以便开始监控 ONTAP 系统。

开始之前

- 如果这是您第一次访问 Web UI，则必须以维护用户（或 Linux 安装的 umadmin 用户）身份登录。
- 如果您计划允许用户使用短名称而不是使用完全限定的域名（FQDN）或 IP 地址访问 Unified Manager，则您的网络配置必须将此短名称解析为有效的 FQDN。
- 如果服务器使用自签名数字证书，则浏览器可能会显示警告，指示该证书不受信任。您可以确认风险并继续访问，也可以安装用于服务器身份验证的证书颁发机构（CA）签名的数字证书。

步骤

1. 请使用安装结束时显示的 URL 从浏览器启动 Unified Manager Web UI。该 URL 是 Unified Manager 服务器的 IP 地址或完全限定域名（FQDN）。

链接的格式如下： `https://URL`。

2. 使用维护用户凭据登录到 Unified Manager Web UI。

> 如果您在一小时内连续三次尝试登录 Web UI 失败，您将被系统锁定，并且需要联系您的系统管理员。这仅适用于本地用户。

执行 **Active IQ Unified Manager Web UI** 的初始设置

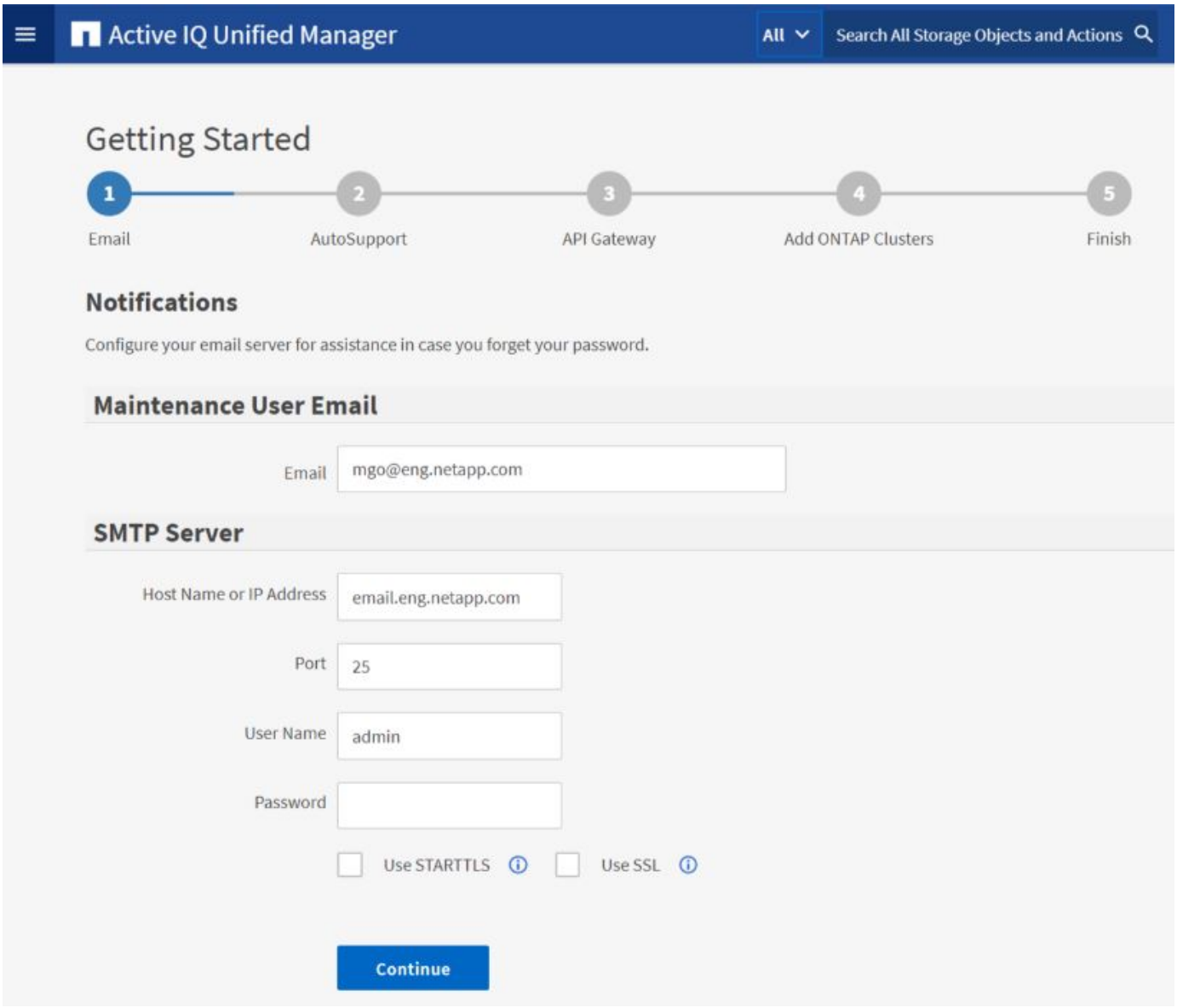
要使用 Unified Manager，必须首先配置初始设置选项，包括 NTP 服务器、维护用户电子邮件地址、SMTP 服务器主机和添加 ONTAP 群集。

开始之前

您必须已执行以下操作：

- 使用安装后提供的 URL 启动 Unified Manager Web UI
- 使用在安装期间创建的维护用户名和密码（对于 Linux 安装，为 umadmin 用户）登录

仅当您首次访问 Web UI 时，才会显示 Active IQ Unified ManagerGetting Started 页面。下面的页面来自 VMware 上的安装。



如果稍后要更改其中任何选项，您可以从 Unified Manager 左侧导航窗格的常规选项中进行选择。请注意，NTP 设置仅适用于 VMware 安装，稍后可以使用 Unified Manager 维护控制台进行更改。

步骤

1. 在“Active IQ Unified Manager 初始设置”页面中，输入维护用户电子邮件地址、SMTP 服务器主机名和任何其他 SMTP 选项，以及 NTP 服务器（仅限 VMware 安装）。然后单击 继续。

   如果您选择了 使用 **STARTTLS** 或 使用 **SSL** 选项，则单击 继续 按钮后会显示证书页面。验证证书详细信息并接受证书以继续进行 Web UI 的初始设置。

2. 在 AutoSupport 页面中，单击 **Agree and Continue** 以启用从 Unified Manager 向 NetAppActive IQ 发送 AutoSupport 消息的功能。

   如果需要指定代理来提供 Internet 访问以发送 AutoSupport 内容，或者如果要禁用 AutoSupport，请使用 Web UI 中的 **General** > **AutoSupport** 选项。

3. 在 Red Hat 系统上，将 umadmin 用户密码从默认的“`admin`”字符串更改为个性化字符串。

4. 在 Set up API Gateway 页面中，选择是否要使用 API Gateway 功能，该功能允许 Active IQ Unified Manager 使用 ONTAP REST API 管理您计划监控的 ONTAP 集群。然后单击 **Continue**。

   您可以稍后在 Web UI 中从 常规 > 功能设置 > **API** 网关 启用或禁用此设置。有关 API 的详细信息，请参见 "Active IQ Unified Manager REST API 入门"。

5. 添加您希望 Unified Manager 管理的集群，然后单击 下一步。对于您计划管理的每个集群，您必须具有主机名或集群管理 IP 地址（IPv4 或 IPv6）以及用户名和密码凭据——用户必须具有“admin”角色。

   此步骤为可选步骤。您可以稍后在 Web UI 中从 存储管理 > 集群设置 添加集群。

6. 在“摘要”页面中，验证所有设置是否正确，然后单击 完成。

“入门”页面关闭并显示“Unified Manager 仪表板”页面。

向 **Active IQ Unified Manager** 添加集群

您可以将集群添加到 Active IQ Unified Manager 以便可以监视该集群。这包括能够获取集群信息，例如集群的运行状况、容量、性能和配置，以便您可以查找并解决可能发生的任何问题。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须具有下列信息：
  - Unified Manager 支持本地 ONTAP 集群、ONTAP Select、Cloud Volumes ONTAP。
  - 主机名或集群管理 IP 地址

    主机名是 FQDN 或 Unified Manager 用来连接集群的简称。主机名必须解析为集群管理 IP 地址。

    集群管理 IP 地址必须是管理存储虚拟机（SVM）的集群管理 LIF。如果使用节点管理 LIF，则操作会失败。

  - 此集群必须运行 ONTAP 9.1 或更高版本的软件。
  - ONTAP 管理员用户名和密码

    此帐户必须具有 *admin* 角色，应用程序访问权限设置为 *ontapi*、*amqp*、*console* 和 *http*。

  - 使用 HTTPS 协议连接到集群的端口号（通常为端口 443）
  - 您拥有所需的证书：

    SSL (HTTPS) 证书：此证书由 Unified Manager 拥有。全新安装 Unified Manager 时，会生成默认的自签名 SSL (HTTPS) 证书。NetApp 建议将其升级为 CA 签名证书，以获得更好的安全性。如果服务器证书过期，您应重新生成该证书并重新启动 Unified Manager，以便服务采用新证书。有关重新生成 SSL 证书的详细信息，请参见 "生成 HTTPS 安全证书"。

    EMS 证书：此证书归 Unified Manager 所有。它在对从 ONTAP 接收的 EMS 通知进行身份验证时使用。

    双向 **TLS** 通信证书：在 Unified Manager 和 ONTAP 之间的双向 TLS 通信期间使用。系统会根据

ONTAP 版本为集群启用基于证书的身份验证。如果集群运行的 ONTAP 版本低于 9.5，则不会启用基于证书的身份验证。

如果您要更新早期版本的 Unified Manager，则不会为集群自动启用基于证书的身份验证。但是，您可以通过修改并保存集群详细信息来启用它。如果证书过期，您应重新生成证书以整合新证书。有关查看和重新生成证书的详细信息，请参见"编辑集群"。

- 您可以从 Web UI 添加集群，并自动启用基于证书的身份验证。
- 您可以通过 Unified Manager CLI 添加集群，默认情况下不会启用基于证书的身份验证。如果使用 Unified Manager CLI 添加集群，则需要使用 Unified Manager UI 编辑集群。您可以查看 "支持的 Unified Manager CLI 命令" 了解如何使用 Unified Manager CLI 添加集群。
- 如果为集群启用了基于证书的身份验证，并且您从服务器获取 Unified Manager 的备份并还原到主机名或 IP 地址已更改的另一台 Unified Manager 服务器，则对集群的监控可能会失败。为避免失败，请编辑并保存集群详细信息。有关编辑集群详细信息的更多信息，请参见 "编辑集群"。

+
集群证书：此证书归 ONTAP 所有。您无法将证书已过期的集群添加到 Unified Manager，如果证书已过期，则应在添加集群之前重新生成该证书。有关证书生成的信息，请参见知识库（KB）文章 "如何在 System Manager 用户界面中续订 ONTAP 自签名证书"。

- 您必须在 Unified Manager 服务器上有足够的空间。当数据库目录中超过 90% 的空间已被占用时，您将无法向服务器添加集群。

对于 MetroCluster 配置，必须同时添加本地和远程集群，并且必须正确配置集群。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 集群设置。
2. 在“集群设置”页面上，单击*添加*。
3. 在添加群集对话框中，指定所需的值，例如群集的主机名或 IP 地址、用户名、密码和端口号。

   您可以将集群管理 IP 地址从 IPv6 更改为 IPv4，或者从 IPv4 更改为 IPv6。下一个监控周期完成后，新的 IP 地址将反映在集群网格和集群配置页面中。
4. 单击*提交*。
5. 在 Authorize Host 对话框中，单击 **View Certificate** 可查看集群的证书信息。
6. 单击 **Yes**。

   保存集群详细信息后，可以查看集群的 Mutual TLS 通信证书。

   如果未启用基于证书的身份验证，Unified Manager 仅在最初添加集群时检查证书。Unified Manager 不会检查对 ONTAP 的每次 API 调用的证书。

发现新集群的所有对象后，Unified Manager 将开始收集前 15 天的历史性能数据。这些统计数据通过数据连续性收集功能进行收集。此功能可在集群添加后立即为您提供超过两周的集群性能信息。数据连续性收集周期完成后，将默认每五分钟收集一次实时集群性能数据。

由于收集 15 天的性能数据是 CPU 密集型的，因此建议您错开添加新集群，以便数据连续性收集

轮询不会同时在太多集群上运行。此外，如果您在数据连续性收集期间重新启动 Unified Manager，则收集将暂停，您将看到缺失时间范围内的性能图表中的缺口。

如果收到无法添加集群的错误消息，请检查两个系统上的时钟是否未同步，以及 Unified Manager HTTPS 证书开始日期是否晚于集群上的日期。您必须确保时钟使用 NTP 或类似服务进行同步。

相关信息

"安装 CA 签名并返回的 HTTPS 证书"

配置通知

配置 **Active IQ Unified Manager** 以发送警报通知

您可以将 Unified Manager 配置为发送通知，提醒您环境中的事件。在发送通知之前，必须配置多个其他 Unified Manager 选项。

开始之前

您必须具有应用程序管理员角色。

部署 Unified Manager 并完成初始配置后，应考虑配置环境以触发警报，并根据接收到的事件生成通知电子邮件或 SNMP 陷阱。

步骤

1. "配置事件通知设置"。

   如果要在环境中发生某些事件时发送警报通知，则必须配置 SMTP 服务器并提供用于发送警报通知的电子邮件地址。如果要使用 SNMP 陷阱，可以选择该选项并提供必要的信息。

2. "启用远程身份验证"。

   如果希望远程 LDAP 或 Active Directory 用户访问 Unified Manager 实例并接收警报通知，则必须启用远程身份验证。

3. "添加身份验证服务器"。

   您可以添加身份验证服务器，以便身份验证服务器中的远程用户可以访问 Unified Manager。

4. "添加用户"。

   您可以添加几种不同类型的本地或远程用户并分配特定角色。在您创建警报时，您需要指定一个用户来接收警报通知。

5. "添加警报"。

   添加发送通知的电子邮件地址，添加接收通知的用户，配置网络设置，以及配置环境所需的 SMTP 和 SNMP 选项后，即可分配警报。

在 **Active IQ Unified Manager** 中配置事件通知设置

您可以将 Unified Manager 配置为在生成事件或将事件分配给用户时发送警报通知。您可以配置用于发送警报的 SMTP 服务器，也可以设置各种通知机制——例如，警报通知可以作为电子邮件或 SNMP 陷阱发送。

开始之前

您必须具有下列信息：

- 发送警报通知的电子邮件地址

  电子邮件地址显示在发送的警报通知中的“From”字段中。如果由于任何原因无法发送电子邮件，此电子邮件地址也将用作无法投递邮件的收件人。

- SMTP 服务器主机名，以及访问服务器的用户名和密码
- 将接收 SNMP 陷阱的陷阱目标主机的主机名或 IP 地址，以及 SNMP 版本、出站陷阱端口、团体和其他必需的 SNMP 配置值

  要指定多个陷阱目标，请使用逗号分隔每个主机。在这种情况下，所有其他 SNMP 设置（例如版本和出站陷阱端口）必须对于此列表中的所有主机都相同。

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*常规* > 通知。
2. 在“通知”页面中，配置适当的设置。

   备注：

   - 如果发件人地址预先填写了地址“ActiveIQUnifiedManager@localhost.com”，则应将其更改为真实有效的电子邮件地址，以确保所有电子邮件通知都能成功发送。
   - 如果无法解析 SMTP 服务器的主机名，则可以指定 SMTP 服务器的 IP 地址（IPv4 或 IPv6）而不是主机名。
3. 单击 **Save**。
4. 如果您选择了 使用 **STARTTLS** 或 使用 **SSL** 选项，则单击 保存 按钮后会显示证书页面。验证证书详细信息并接受证书以保存通知设置。

   您可以单击*查看证书详细信息*按钮以查看证书详细信息。如果现有证书已过期，请取消选中*使用 STARTTLS*或*使用 SSL*复选框，保存通知设置，然后再次选中*使用 STARTTLS*或*使用 SSL*复选框以查看新证书。

在 **Active IQ Unified Manager** 中启用远程身份验证

您可以启用远程身份验证，以便 Unified Manager 服务器可以与您的身份验证服务器通信。身份验证服务器的用户可以访问 Unified Manager 图形界面来管理存储对象和数据。

开始之前

您必须具有应用程序管理员角色。

Unified Manager 服务器必须直接连接到身份验证服务器。您必须禁用任何本地 LDAP 客户端，例如 SSSD（系统安全服务后台程序）或 NSLCD（名称服务 LDAP 缓存后台程序）。

您可以使用 Open LDAP 或 Active Directory 启用远程身份验证。如果禁用远程身份验证，远程用户将无法访问 Unified Manager。

支持通过 LDAP 和 LDAPS（安全 LDAP）进行远程身份验证。Unified Manager 使用 389 作为非安全通信的默认端口，636 作为安全通信的默认端口。

用于对用户进行身份验证的证书必须符合 X.509 格式。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 选中*启用远程身份验证……*的复选框。
3. 在身份验证服务字段中，选择服务类型并配置身份验证服务。

对于身份验证类型……	输入以下信息……
Active Directory	• 以下格式之一的身份验证服务器管理员名称： ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` （使用适当的 LDAP 表示法） • 管理员密码 • 基本可分辨名称（使用适当的 LDAP 表示法）
打开 LDAP	• 绑定可分辨名称（使用适当的 LDAP 表示法） • 绑定密码 • 基本可分辨名称

如果 Active Directory 用户的身份验证需要很长时间或超时，则身份验证服务器可能需要很长时间才能响应。在 Unified Manager 中禁用对嵌套组的支持可能会缩短身份验证时间。

如果为身份验证服务器选择使用安全连接选项，则 Unified Manager 将使用安全套接字层（SSL）协议与身份验证服务器进行通信。

4. 可选： 添加身份验证服务器，并测试身份验证。
5. 单击 **Save**。

在 **Active IQ Unified Manager** 中禁用远程身份验证中的嵌套组

如果启用了远程身份验证，则可以禁用嵌套组身份验证，以便只有单个用户（而不是组成员）可以对 Unified Manager 进行远程身份验证。如果要改善 Active Directory 身份验证响应时间，则可以禁用嵌套组。

开始之前

- 您必须具有应用程序管理员角色。
- 禁用嵌套组仅适用于使用 Active Directory 时。

禁用对 Unified Manager 中嵌套组的支持可能会缩短身份验证时间。如果禁用嵌套组支持，并且将远程组添加到 Unified Manager，则单个用户必须是远程组的成员才能向 Unified Manager 进行身份验证。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 选中*禁用嵌套组查找*复选框。
3. 单击 **Save**。

在 **Active IQ Unified Manager** 中设置身份验证服务

身份验证服务在向身份验证服务器中的远程用户或远程组提供对 Unified Manager 的访问权限之前对其进行身份验证。可以通过使用预定义的身份验证服务（如 Active Directory 或 OpenLDAP）或配置自己的身份验证机制来对用户进行身份验证。

开始之前

- 您必须已启用远程身份验证。
- 您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 从下列身份验证服务中选择一项：

如果选择……	操作
Active Directory	a. 输入管理员名称和密码。 b. 指定身份验证服务器的基本可分辨名称。 例如，如果身份验证服务器的域名为+ou@domain.com+，则基本可分辨名称为*cn=ou,dc=domain,dc=com*。
OpenLDAP	a. 输入绑定可分辨名称和绑定密码。 b. 指定身份验证服务器的基本可分辨名称。 例如，如果身份验证服务器的域名为+ou@domain.com+，则基本可分辨名称为*cn=ou,dc=domain,dc=com*。

如果选择.....	操作
其他	a. 输入绑定可分辨名称和绑定密码。 b. 指定身份验证服务器的基本可分辨名称。 例如，如果身份验证服务器的域名为+ou@domain.com+，则基本可分辨名称为*cn=ou,dc=domain,dc=com*。 c. 指定身份验证服务器支持的 LDAP 协议版本。 d. 输入用户名、组成员身份、用户组和成员属性。

如果要修改身份验证服务，则必须删除所有现有的身份验证服务器，然后添加新的身份验证服务器。

3. 单击 **Save**。

向 **Active IQ Unified Manager** 添加身份验证服务器

可以在管理服务器上添加身份验证服务器并启用远程身份验证，以便身份验证服务器中的远程用户可以访问 Unified Manager。

开始之前

- 必须提供以下信息：
  - 身份验证服务器的主机名或 IP 地址
  - 身份验证服务器的端口号
- 必须已启用远程身份验证并配置身份验证服务，以便管理服务器可以对身份验证服务器中的远程用户或组进行身份验证。
- 您必须具有应用程序管理员角色。

如果要添加的身份验证服务器是高可用性（HA）对的一部分（使用相同的数据库），则还可以添加配对身份验证服务器。这样，当其中一个身份验证服务器无法访问时，管理服务器便可以与配对服务器进行通信。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 启用或禁用*使用安全连接*选项：

目的	操作
启用	a. 选择*使用安全连接*选项。 b. 在身份验证服务器区域中，单击 添加。 c. 在“添加身份验证服务器”对话框中，输入服务器的身份验证名称或 IP 地址（IPv4 或 IPv6）。 d. 在 Authorize Host 对话框中，单击 View Certificate。 e. 在查看证书对话框中，验证证书信息，然后单击*关闭*。 f. 在 Authorize Host 对话框中，单击 **Yes**。 启用 使用安全连接身份验证 选项时，Unified Manager 将与身份验证服务器通信并显示证书。Unified Manager 使用 636 作为安全通信的默认端口，端口号 389 用于非安全通信。
禁用	a. 清除*使用安全连接*选项。 b. 在身份验证服务器区域中，单击 添加。 c. 在“添加身份验证服务器”对话框中，指定服务器的主机名或 IP 地址（IPv4 或 IPv6）以及端口详细信息。 d. 单击 **Add**。

已添加的身份验证服务器将显示在“服务器”区域中。

3. 执行测试身份验证以确认可以对添加的身份验证服务器中的用户进行身份验证。

测试 **Active IQ Unified Manager** 中身份验证服务器的配置

您可以验证身份验证服务器的配置，以确保管理服务器能够与其通信。您可以通过从身份验证服务器搜索远程用户或远程组并使用配置的设置对其进行身份验证来验证配置。

开始之前

- 必须已启用远程身份验证并配置身份验证服务，以便 Unified Manager 服务器可以对远程用户或远程组进行身份验证。
- 您必须已添加身份验证服务器，以便管理服务器可以从这些服务器中搜索远程用户或远程组并对其进行身份验证。
- 您必须具有应用程序管理员角色。

如果身份验证服务设置为 Active Directory，并且正在验证属于身份验证服务器主组的远程用户的身份验证，则身份验证结果中不会显示有关主组的信息。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 单击*测试身份验证*。
3. 在 Test User 对话框中，指定远程用户的用户名和密码或远程组的用户名，然后单击 **Test**。

   如果要对远程组进行身份验证，则不得输入密码。

在 **Active IQ Unified Manager** 中添加警报

您可以配置警报，以便在生成特定事件时通知您。可以为单个资源、一组资源或特定严重性类型的事件配置警报。您可以指定要收到通知的频率，并将脚本关联到警报。

开始之前

- 您必须配置通知设置（如用户电子邮件地址、SMTP 服务器和 SNMP 陷阱主机），以使 Active IQ Unified Manager 服务器能够在生成事件时使用这些设置向用户发送通知。
- 您必须知道要触发警报的资源和事件，以及要通知的用户的用户名或电子邮件地址。
- 如果要根据事件执行脚本，则必须使用“脚本”页面将脚本添加到 Unified Manager。
- 您必须具有应用程序管理员或存储管理员角色。

除了从“警报设置”页面创建警报之外，您还可以在收到事件后直接从“事件详细信息”页面创建警报，如此处所述。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。
2. 在警报设置页面中，单击*添加*。
3. 在添加警报对话框中，单击*名称*，并输入警报的名称和描述。
4. 单击*资源*，然后选择要包含在此警报中或从此警报中排除的资源。

   您可以通过在*名称包含*字段中指定文本字符串来设置筛选器，以选择一组资源。根据指定的文本字符串，可用资源列表仅显示与筛选规则匹配的资源。指定的文本字符串区分大小写。

   如果资源同时符合已指定的包含和排除规则，则排除规则优先于包含规则，并且不会为与排除资源相关的事件生成警报。

5. 单击*事件*，并根据要触发警报的事件名称或事件严重性类型选择事件。

   要选择多个事件，请在进行选择时按 Ctrl 键。

6. 单击 操作，选择要通知的用户，选择通知频率，选择是否将 SNMP 陷阱发送到陷阱接收器，并分配生成警报时要执行的脚本。

   如果修改为用户指定的电子邮件地址并重新打开警报进行编辑，则“名称”字段将显示为空白，因为修改后的电子邮件地址不再映射到先前选择的用户。此外，如果从“用户”页面修改了所选用户的电子邮件地址，则不会为所选用户更新已修改的电子邮件地址。

   您也可以选择通过 SNMP 陷阱通知用户。

7. 单击 **Save**。

添加警报的示例

此示例演示如何创建满足以下要求的警报：

- 警报名称：HealthTest
- 资源：包括名称中含有 “abc” 的所有卷，并排除名称中含有 “xyz” 的所有卷
- 事件：包括所有严重运行状况事件
- 操作：包括 "sample@domain.com"、一个 “Test” 脚本，并且必须每 15 分钟通知一次用户

请在添加警报对话框中执行以下步骤：

步骤

1. 单击*名称*，然后在*警报名称*字段中输入*HealthTest*。
2. 单击*资源*，然后在包含选项卡中，从下拉列表中选择*卷*。
   a. 在 名称包含 字段中输入 **abc** 以显示名称包含 “abc” 的卷。
   b. 从可用资源区域中选择 **<<All Volumes whose name contains 'abc'>>**，并将其移动到选定资源区域。
   c. 单击*排除*，然后在*名称包含*字段中输入*xyz*，然后单击*添加*。
3. 单击*事件*，然后从事件严重性字段中选择*严重*。
4. 从"匹配事件"区域中选择 **All Critical Events**，然后将其移动到"已选择事件"区域。
5. 单击 操作，并在提醒这些用户字段中输入 **sample@domain.com**。
6. 选择*每 15 分钟提醒一次*，每 15 分钟通知一次用户。

   您可以将警报配置为在指定时间内重复向收件人发送通知。您应确定警报的事件通知处于活动状态的时间。

7. 在“Select Script to Execute”菜单中，选择 **Test** 脚本。
8. 单击 **Save**。

在 Active IQ Unified Manager 中更改本地用户密码

您可以更改本地用户登录密码，以避免出现可能的安全风险。

开始之前

必须以本地用户身份登录。

无法使用这些步骤更改维护用户和远程用户的密码。要更改远程用户密码，请联系您的密码管理员。要更改维护用户密码，请参阅 "使用维护控制台"。

步骤

1. 登录到 Unified Manager。
2. 在顶部菜单栏中，单击用户图标，然后单击*更改密码*。

   如果您是远程用户，则不会显示*更改密码*选项。

3. 在"更改密码"对话框中，输入当前密码和新密码。
4. 单击 **Save**。

如果在高可用性配置中配置了 Unified Manager，则必须在设置的第二个节点上更改密码。两个实例必须具有相同的密码。

在 **Active IQ Unified Manager** 中设置会话非活动超时

您可以为 Unified Manager 指定非活动超时值，以便在一段时间非活动后自动终止会话。默认情况下，超时设置为 4,320 分钟（72 小时）。

开始之前

您必须具有应用程序管理员角色。

此设置会影响所有登录的用户会话。

如果已启用安全断言标记语言（SAML）身份验证，则此选项不可用。

步骤

1. 在左侧导航窗格中，单击*常规* > 功能设置。
2. 在*功能设置*页面中，通过选择以下选项之一指定非活动超时：

目的	操作
未设置超时，因此会话永远不会自动关闭	在*非活动超时*面板中，将滑块按钮向左移动（关闭），然后单击*应用*。
设置特定的分钟数作为超时值	在*非活动超时*面板中，将滑块按钮向右移动（开启），以分钟为单位指定非活动超时值，然后单击*应用*。

使用 **Active IQ Unified Manager** 中的 **CLI** 设置会话超时

您可以使用 CLI 为 Unified Manager 设置最大会话超时值，以便在一段时间后自动终止会话。默认情况下，您的会话超时设置为最大值，即 4,320 分钟（72 小时）。这意味着您的会话将在 72 小时后自动结束，即使您已登录并正在积极使用 Unified Manager 也是如此。

关于此任务

您必须具有应用程序管理员角色。

会话超时设置会影响所有登录的用户会话。

步骤

1. 输入 `um cli login`命令登录到 Unified Manager CLI。使用有效的用户名和密码进行身份验证。
2. 输入 `um option set max.session.timeout.value=<in mins>`命令以修改会话超时值。

更改 Unified Manager 主机名

更改 Active IQ Unified Manager 虚拟设备主机名

首次部署 Unified Manager 虚拟设备时，将为网络主机分配一个名称。可以在部署后更改主机名。如果更改主机名，则还必须重新生成 HTTPS 证书。

开始之前

您必须以维护用户身份登录到 Unified Manager，或者拥有应用程序管理员角色，才能执行这些任务。

您可以使用主机名（或主机 IP 地址）访问 Unified Manager Web UI。如果在部署期间为网络配置了静态 IP 地址，则会为网络主机指定名称。如果使用 DHCP 配置网络，则主机名应取自 DNS。如果未正确配置 DHCP 或 DNS，则会自动分配主机名“`Unified Manager`”，并将其与安全证书相关联。

无论主机名是如何分配的，如果更改主机名并打算使用新主机名访问 Unified Manager Web UI，则必须生成新的安全证书。

如果使用服务器的 IP 地址而不是主机名访问 Web UI，那么在更改主机名时，无需生成新证书。但是，最佳做法是更新证书，使证书中的主机名与实际主机名相匹配。

如果在 Unified Manager 中更改主机名，则必须在 OnCommand Workflow Automation (WFA) 中手动更新主机名。WFA 中的主机名不会自动更新。

在重新启动 Unified Manager 虚拟机之前，新证书不会生效。

步骤

1. 生成 HTTPS 安全证书

   如果要使用新主机名访问 Unified Manager Web UI，则必须重新生成 HTTPS 证书以将其与新主机名关联。

2. 重新启动 Unified Manager 虚拟机

   重新生成 HTTPS 证书后，必须重新启动 Unified Manager 虚拟机。

在 Active IQ Unified Manager 中生成 HTTPS 安全证书

首次安装 Active IQ Unified Manager 时，将安装默认 HTTPS 证书。您可能会生成一个新的 HTTPS 安全证书来替换现有证书。

开始之前

您必须具有应用程序管理员角色。

重新生成证书的原因可能有多种，例如希望为可分辨名称 （DN） 设置更好的值、希望使用更大的密钥大小、更长的有效期，或者当前证书已过期。

如果无权访问 Unified Manager Web UI，则可以使用维护控制台使用相同的值重新生成 HTTPS 证书。在重新生成证书时，您可以定义密钥大小和密钥的有效期。如果使用维护控制台中的 `Reset Server Certificate`选项，则会创建一个有效期为 397 天的新 HTTPS 证书。此证书将具有大小为 2048 位的 RSA 密钥。

步骤

1. 在左侧导航窗格中，单击 常规 > **HTTPS** 证书。
2. 单击 重新生成 **HTTPS** 证书。

   此时将显示重新生成 HTTPS 证书对话框。

3. 根据您要生成证书的方式选择以下选项之一：

目的	操作
使用当前值重新生成证书	单击*使用当前证书属性重新生成*选项。
使用其他值生成证书	单击*更新当前证书属性*选项。 如果不输入新值，Common Name 和 Alternative Names 字段将使用现有证书中的值。“Common Name”应设置为主机的 FQDN。其他字段不需要值，但如果希望在证书中填充这些值，则可以输入值，例如 EMAIL、COMPANY、DEPARTMENT、City 、State 和 Country 的值。您还可以从可用的 KEY SIZE（密钥算法为“RSA”。）和 VALIDITY PERIOD 中进行选择。 • 密钥大小的允许值为 2048、3072`和 `4096。 • 有效期为最少 1 天至最多 36500 天。 即使允许 36500 天的有效期，也建议您使用不超过 397 天或 13 个月的有效期。因为如果您选择了超过 397 天的有效期，并计划导出此证书的 CSR 并由知名的 CA 签名，则 CA 退还给您的签名证书的有效期将缩短至 397 天。 • 如果要从证书的 Alternative Names 字段中删除本地标识信息，可以选中“排除本地标识信息（例如 localhost）”复选框。选中此复选框时，Alternative Names 字段中将仅使用您在该字段中输入的内容。如果留空，生成的证书将完全没有 Alternative Names 字段。

4. 单击*是*以重新生成证书。
5. 重新启动 Unified Manager 服务器以使新证书生效。
6. 通过查看 HTTPS 证书，可验证新证书的信息。

重新启动 **Active IQ Unified Manager** 虚拟机

您可以从 Unified Manager 的维护控制台重新启动虚拟机。在生成新的安全证书后，或者如果虚拟机出现问题，您必须重新启动。

开始之前

已打开虚拟设备的电源。

您以维护用户身份登录到维护控制台。

您还可以使用 **Restart Guest** 选项从 vSphere 重新启动虚拟机。有关详细信息，请参见 VMware 文档。

步骤

1. 访问维护控制台。
2. 选择*系统配置* > 重启虚拟机。

在 **Linux** 系统上更改 **Active IQ Unified Manager** 主机名

在某些时候，您可能需要更改已安装 Unified Manager 的 Red Hat Enterprise Linux 计算机的主机名。例如，您可能希望在列出 Linux 计算机时按类型、工作组或受监视的集群组重命名主机，以便更轻松地识别 Unified Manager 服务器。

开始之前

您必须具有对安装了 Unified Manager 的 Linux 系统的 root 用户访问权限。

您可以使用主机名（或主机 IP 地址）访问 Unified Manager web UI。如果在部署期间为网络配置了静态 IP 地址，则会为网络主机指定一个名称。如果使用 DHCP 配置网络，则应从 DNS 服务器获取主机名。

无论主机名是如何分配的，如果更改主机名并打算使用新主机名来访问 Unified Manager Web UI，则必须生成新的安全证书。

如果使用服务器的 IP 地址而不是主机名访问 web UI，则在更改主机名时无需生成新证书。但是，最佳做法是更新证书，以便证书中的主机名与实际主机名相匹配。重新启动 Linux 计算机之前，新证书不会生效。

如果在 Unified Manager 中更改主机名，则必须在 OnCommand Workflow Automation (WFA) 中手动更新主机名。WFA 中的主机名不会自动更新。

步骤

1. 以 root 用户身份登录到要修改的 Unified Manager 系统。
2. 通过输入以下命令停止 Unified Manager 软件和相关的 MySQL 软件：

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. 使用 Linux `hostnamectl` 命令更改主机名：

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. 重新生成服务器的 HTTPS 证书：

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. 重新启动网络服务：

   ```
   systemctl restart NetworkManager.service
   ```

6. 服务重新启动后，验证新主机名是否能够 ping 通自己：

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   此命令应返回之前为原始主机名设置的相同 IP 地址。

7. 完成并验证主机名更改后，通过输入以下命令重新启动 Unified Manager：

   ```
   systemctl start mysqld ocie ocieau
   ```

在 **Active IQ Unified Manager** 中启用和禁用基于策略的存储管理

从 Unified Manager 9.7 开始，您可以在 ONTAP 集群上配置存储工作负载（卷和 LUN），并根据分配的性能服务级别管理这些工作负载。此功能类似于在 ONTAP System Manager 中创建工作负载并附加 QoS 策略，但使用 Unified Manager 应用时，您可以在 Unified Manager 实例正在监控的所有集群中配置和管理工作负载。

您必须具有应用程序管理员角色。

默认情况下，此选项处于启用状态，但如果您不想使用 Unified Manager 配置和管理工作负载，则可以将其禁用。

启用后，此选项将在用户界面中提供许多新项目：

新内容	位置
配置新工作负载的页面	可从 **Common Tasks** > **Provisioning** 获得
用于创建性能服务级别策略的页面	可从 设置 > 策略 > 性能服务级别 中获取
用于创建性能存储效率策略的页面	可从*设置* > 策略 > 存储效率
描述当前工作负载性能和工作负载 IOPS 的面板	可从信息板获得

有关这些页面和此功能的更多信息，请参见产品中的联机帮助。

步骤

1. 在左侧导航窗格中，单击*常规* > 功能设置。
2. 在*功能设置*页面中，通过选择以下选项之一禁用或启用基于策略的存储管理：

目的	操作
禁用基于策略的存储管理	在*基于策略的存储管理*面板中，向左移动滑块按钮。
启用基于策略的存储管理	在*基于策略的存储管理*面板中，将滑块按钮向右移动。

配置 Active IQ Unified Manager 备份

您可以通过在主机系统上和通过维护控制台执行的一组配置步骤，在 Unified Manager 上配置备份功能。

有关配置步骤的信息，请参见 "管理备份和还原操作"。

管理功能设置

了解 Active IQ Unified Manager 中的功能设置

“功能设置”页面允许您在 Active IQ Unified Manager 中启用和禁用特定功能。这包括根据策略创建和管理存储对象、启用 API 网关和登录横幅、上传用于管理警报的脚本、根据非活动时间使 Web UI 会话超时，以及禁用接收 Active IQ 平台事件。

“功能设置”页面仅适用于具有应用程序管理员角色的用户。

有关脚本上传的信息，请参见 "启用和禁用脚本上传"。

在 Active IQ Unified Manager 中启用基于策略的存储管理

*基于策略的存储管理*选项允许基于服务级别目标（SLO）进行存储管理。默认情况下，此选项处于启用状态。

激活此功能后，您可以在添加到 Active IQ Unified Manager 实例的 ONTAP 集群上配置存储工作负载，并根据分配的性能服务级别和存储效率策略管理这些工作负载。

您可以从*常规* > 功能设置 > *基于策略的存储管理*中选择激活或停用此功能。激活此功能后，以下页面可用于操作和监控：

- 配置（存储工作负载配置）
- 策略 > 性能服务级别
- 策略 > 存储效率
- “群集设置”页面上的“通过性能服务级别管理的工作负载”列
- *仪表板*上的工作负载性能面板

您可以使用这些屏幕创建性能服务级别和存储效率策略，并配置存储工作负载。您还可以监控符合已分配性能服务级别的存储工作负载，以及不符合的存储工作负载。工作负载性能和工作负载 IOPS 面板还可让您根据在集群上配置的存储工作负载，评估数据中心内各集群的总容量、可用容量和已用容量以及性能 （IOPS）。

激活此功能后，您可以运行 Unified Manager REST API，以执行 菜单栏 > 帮助按钮 > **API** 文档 > **storage-provider** 类别中的某些功能。或者，您可以输入主机名或 IP 地址以及用于访问 REST API 页面的 URL，格式为 https://<hostname>/docs/api/

有关 API 的详细信息，请参见 "Active IQ Unified Manager REST API 入门"。

了解 **Active IQ Unified Manager** 中的 **API Gateway** 功能

API 网关功能使 Active IQ Unified Manager 成为单一控制平面，您可以从中管理多个 ONTAP 集群，而无需单独登录到这些集群。

您可以从首次登录到 Unified Manager 时显示的配置页面启用此功能。或者，您可以从 常规 > 功能设置 > **API** 网关 启用或禁用此功能。

Unified Manager REST API 与 ONTAP REST API 不同，并且并非 ONTAP REST API 的所有功能都可以通过使用 Unified Manager REST API 来实现。但是，如果您有访问 ONTAP API 以管理未向 Unified Manager 公开的特定功能的特定业务需求，则可以启用 API 网关功能并执行 ONTAP API。网关充当代理，通过以与 ONTAP API 相同的格式维护标头和正文请求来隧道传输 API 请求。您可以使用 Unified Manager 凭据并执行特定 API 以访问和管理 ONTAP 集群，而无需传递各个集群凭据。Unified Manager 作为单点管理，用于在由您的 Unified Manager 实例管理的 ONTAP 集群中运行 API。API 返回的响应与直接从 ONTAP 执行的相应 ONTAP REST API 返回的响应相同。

启用此功能后，您可以从*菜单栏* > 帮助按钮 > **API** 文档 > *网关*类别执行 Unified Manager REST API。或者，您可以按以下格式输入主机名或 IP 地址以及用于访问 REST API 页面的 URL `https://<hostname>/docs/api/`

有关 API 的详细信息，请参见 "Active IQ Unified Manager REST API 入门"。

在 **Active IQ Unified Manager** 中指定非活动超时

您可以为 Active IQ Unified Manager 指定非活动超时值。在指定时间处于非活动状态后，应用程序将自动注销。默认情况下，此选项处于启用状态。

您可以在 常规 > 功能设置 > 非活动超时 中停用此功能或修改时间。激活此功能后，应在 **LOGOUT AFTER** 字段中指定非活动时间限制（以分钟为单位），之后系统会自动注销。默认值为 4320 分钟（72 小时）。

如果已启用安全断言标记语言（SAML）身份验证，则此选项不可用。

在 **Active IQ Unified Manager** 中启用 **Active IQ** 门户事件

您可以指定是否要启用或禁用 Active IQ 门户事件。此设置允许 Active IQ 门户发现并显示有关系统配置、布线等的其他事件。默认情况下，此选项处于启用状态。

启用此功能后，Active IQ Unified Manager 将显示 Active IQ 门户发现的事件。这些事件是通过针对所有受监视的存储系统生成的 AutoSupport 消息运行一组规则来创建的。这些事件与其他 Unified Manager 事件不同，它们可识别与系统配置、布线、最佳实践和可用性问题相关的事件或风险。

您可以从 **General** > **Feature Settings** > **Active IQ Portal Events** 选择激活或停用此功能。在没有外部网络访问的站点中，您必须从 **Storage Management** > **Event Setup** > **Upload Rules** 手动上传规则。

此功能默认处于启用状态。禁用此功能将停止在 Unified Manager 上发现或显示 Active IQ 事件。禁用后，启用此功能可使 Unified Manager 在该集群时区的预定义时间 00:15 接收集群上的 Active IQ 事件。

在 **Active IQ Unified Manager** 中启用和禁用合规性安全设置

通过使用功能设置页面*安全仪表板*面板上的*自定义*按钮，您可以在 Unified Manager 上启用或禁用合规性监控的安全参数。

从此页面启用或禁用的设置控制 Unified Manager 上集群和存储虚拟机的整体合规性状态。根据选择，相应的列在集群清单页面的*安全：所有集群*视图和存储虚拟机清单页面的*安全：所有存储虚拟机*视图中可见。

只有具有管理员角色的用户才能编辑这些设置。

将根据 "NetApp ONTAP 9 安全强化指南" 中定义的建议评估您的 ONTAP 集群、存储虚拟机和卷的安全标准。仪表板上的安全面板和安全页面显示集群、存储虚拟机和卷的默认安全合规性状态。还会为存在安全违规的集群和存储虚拟机生成安全事件并启用管理操作。

自定义安全设置

要自定义适用于您的 ONTAP 环境的合规性监控设置，请执行以下步骤：

步骤

1. 单击*常规>功能设置>安全仪表板>自定义*。此时将显示*自定义安全仪表板设置*弹出窗口。

   您启用或禁用的安全合规性参数会直接影响集群和 Storage VM 屏幕上的默认安全视图、报告和计划报告。如果在修改安全参数之前从这些屏幕上传了 Excel 报告，则下载的 Excel 报告可能会出错。

2. 要启用或禁用 ONTAP 集群的自定义设置，请在*集群*下选择所需的常规设置。有关自定义集群合规性的选项的信息，请参见 "集群合规性类别"。
3. 要启用或禁用存储 VM 的自定义设置，请在 存储 **VM** 下选择所需的常规设置。有关自定义存储 VM 合规性选项的信息，请参见 "Storage VM 合规性类别"。

自定义 **AutoSupport** 和身份验证设置

在 **AutoSupport** 设置 部分，您可以指定是否使用 HTTPS 传输从 ONTAP 发送 AutoSupport 消息。

从*身份验证设置*部分，您可以为默认的 ONTAP 管理员用户启用 Unified Manager 警报。

在 **Active IQ Unified Manager** 中启用和禁用脚本上传

默认情况下，将脚本上传到 Unified Manager 并运行它们的功能处于启用状态。如果您的组织出于安全原因不希望允许此活动，您可以禁用此功能。

开始之前

您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击*常规* > 功能设置。
2. 在*功能设置*页面中，通过选择以下选项之一禁用或启用脚本：

目的	操作
禁用脚本	在*脚本上传*面板中，将滑块按钮向左移动。
启用脚本	在*脚本上传*面板中，将滑块按钮向右移动。

在 **Active IQ Unified Manager** 中添加登录横幅

添加登录横幅使您的组织能够显示任何信息，例如登录和注销期间允许访问系统的人员以及使用条款和条件。

任何用户（例如存储操作员或管理员）都可以在登录、注销和会话超时期间查看此登录横幅弹出窗口。

使用维护控制台

了解 **Active IQ Unified Manager** 中的维护控制台

通过 Unified Manager 维护控制台，您可以维护 Unified Manager 系统上的设置，并进行任何必要的更改以防止出现问题。

根据已安装 Unified Manager 的操作系统，维护控制台提供以下功能：

- 对虚拟设备的任何问题进行故障诊断，尤其是在 Unified Manager Web 界面不可用时
- 升级到较新版本的 Unified Manager
- 生成支持包以发送给技术支持
- 配置网络设置
- 更改维护用户密码
- 连接到外部数据提供程序以发送性能统计信息
- 更改内部性能数据收集
- 从以前备份的版本恢复 Unified Manager 数据库和配置设置。

了解 **Active IQ Unified Manager** 中的维护用户

维护用户是在 Red Hat Enterprise Linux 系统上安装 Unified Manager 期间创建的。维护用户名为“umadmin”用户。维护用户在 Web UI 中具有应用程序管理员角色，并且该用户可以创建后续用户并为其分配角色。

维护用户（即 umadmin 用户）也可以访问 Unified Manager 维护控制台。

Active IQ Unified Manager 中的诊断用户功能

诊断访问的目的是使技术支持能够帮助您进行故障排除，您只应在技术支持指导下使用它。

诊断用户可以在技术支持人员的指导下执行操作系统级别的命令，以进行故障排除。

访问 Active IQ Unified Manager 中的维护控制台

如果 Unified Manager 用户界面未运行，或者需要执行用户界面中不可用的功能，则可以访问维护控制台来管理 Unified Manager 系统。

开始之前

您必须已安装并配置 Unified Manager。

15 分钟不活动后，维护控制台会将您注销。

在 VMware 上安装时，如果已经通过 VMware 控制台以维护用户身份登录，则不能同时使用 Secure Shell 登录。

步骤

1. 按照下面的步骤访问维护控制台：

在此操作系统上……	按照下面的步骤进行操作……
VMware	a. 使用 Secure Shell，连接到 Unified Manager 虚拟设备的 IP 地址或完全限定的域名。 b. 使用您的维护用户名和密码登录到维护控制台。
Linux	a. 使用 Secure Shell，连接到 Unified Manager 系统的 IP 地址或完全限定域名。 b. 使用维护用户 (umadmin) 名称和密码登录到此系统。 c. 输入命令 `maintenance_console`并按 Enter 键。
Windows	a. 使用管理员凭据登录到 Unified Manager 系统。 b. 以 Windows 管理员身份启动 PowerShell。 c. 输入命令 `maintenance_console`并按 Enter 键。

此时将显示 Unified Manager 维护控制台菜单。

使用 Active IQ Unified Manager 中的 vSphere VM 控制台访问维护控制台

如果 Unified Manager 用户界面未运行，或者需要执行用户界面中不可用的功能，则可以访问维护控制台以重新配置虚拟设备。

开始之前

- 您必须是维护用户。
- 必须打开虚拟设备电源才能访问维护控制台。

步骤

1. 在 vSphere 客户端中，找到 Unified Manager 虚拟设备。
2. 单击 **Console** 选项卡。
3. 在控制台窗口内单击以登录。
4. 使用您的用户名和密码登录到维护控制台。

   15 分钟不活动后，维护控制台会将您注销。

维护控制台菜单

了解 **Active IQ Unified Manager** 中的维护控制台菜单

维护控制台由不同的菜单组成，使您可以维护和管理 Unified Manager 服务器的特殊功能和配置设置。

根据已安装 Unified Manager 的操作系统，维护控制台包括以下菜单：

- 升级 Unified Manager（仅限 VMware）
- 网络配置（仅限 VMware）
- 系统配置（仅限 VMware）
  a. 支持/诊断
  b. 重置服务器证书
  c. 重新生成客户端证书
  d. 备份还原
  e. 外部数据提供程序
  f. 性能轮询间隔配置
  g. 禁用 SAML 身份验证
  h. 查看/更改应用程序端口
  i. 调试日志配置
  j. 控制对 MySQL 端口 3306 的访问
  k. 退出

您可以从列表中选择数字来访问特定的菜单选项。例如，对于备份和还原，您可以选择 *4*。

Active IQ Unified Manager 中的网络配置菜单

通过网络配置菜单，您可以管理网络设置。当 Unified Manager 用户界面不可用时，应使

用此菜单。

如果 Unified Manager 安装在 Red Hat Enterprise Linux 或 Microsoft Windows 上，则此菜单不可用。

提供以下菜单选项。

- 显示 **IP** 地址设置

  显示虚拟设备的当前网络设置，包括 IP 地址、网络、广播地址、网络掩码、网关和 DNS 服务器。

- 更改 **IP** 地址设置

  使您能够更改虚拟设备的任何网络设置，包括 IP 地址、网络掩码、网关或 DNS 服务器。如果使用维护控制台将网络设置从 DHCP 切换到静态网络，则无法编辑主机名。您必须选择 提交更改 才能使更改生效。

- 显示域名搜索设置

  显示用于解析主机名的域名搜索列表。

- 更改域名搜索设置

  使您能够在解析主机名时更改要搜索的域名。您必须选择*提交更改*才能使更改生效。

- 显示静态路由

  显示当前静态网络路由。

- 更改静态路由

  使您可以添加或删除静态网络路由。必须选择*提交更改*才能使更改生效。

  - 添加路由

    使您可以添加静态路由。

  - 删除路由

    使您可以删除静态路由。

  - 返回

    带您返回*主菜单*。

  - 退出

    退出维护控制台。

- 禁用网络接口

  禁用任何可用的网络接口。如果只有一个网络接口可用，则无法禁用它。必须选择*提交更改*才能使更改生效。

- 启用网络接口

  启用可用的网络接口。您必须选择*提交更改*才能使更改生效。

- 提交更改

  应用对虚拟设备的网络设置所做的任何更改。您必须选择此选项以实施所做的任何更改，否则不会发生更改。

- **Ping** 主机

  Ping 目标主机以确认 IP 地址更改或 DNS 配置。

- 还原为默认设置

  将所有设置重置为出厂默认值。必须选择*提交更改*才能使更改生效。

- 返回

  带您返回*主菜单*。

- 退出

  退出维护控制台。

使用 **Active IQ Unified Manager** 中的系统配置菜单

系统配置菜单通过提供各种选项，例如查看服务器状态以及重新启动和关闭虚拟机，使您能够管理虚拟设备。

在 Linux 或 Microsoft Windows 系统上安装 Unified Manager 时，此菜单中仅提供 “从 Unified Manager 备份还原” 选项。

提供以下菜单选项：

- 显示服务器状态

  显示当前服务器状态。状态选项包括运行和未运行。

  如果服务器未运行，您可能需要与技术支持联系。

- 重新启动虚拟机

  重新启动虚拟机，停止所有服务。重新启动后，虚拟机和服务将重新启动。

- 关闭虚拟机

  关闭虚拟机，停止所有服务。

  您只能从虚拟机控制台选择此选项。

- 更改**<logged in user>**用户密码

更改当前登录的用户的密码，此用户只能是维护用户。

- 增加数据磁盘大小

  增加虚拟机中数据磁盘（磁盘 3）的大小。

- 增加交换磁盘大小

  增加虚拟机中交换磁盘（磁盘 2）的大小。

- 更改时区

  将时区更改为您的位置。

- 更改 **NTP** 服务器

  更改 NTP 服务器设置，例如 IP 地址或完全限定的域名（FQDN）。

- 更改 **NTP** 服务

  在 `ntp`和 `systemd-timesyncd`服务之间切换。

- 从 **Unified Manager** 备份还原

  从以前备份的版本恢复 Unified Manager 数据库和配置设置。

- 重置服务器证书

  重置服务器安全证书。

- 更改主机名称

  更改安装虚拟设备的主机名称。

- 返回

  退出系统配置菜单并返回主菜单。

- 退出

  退出维护控制台菜单。

使用 **Active IQ Unified Manager** 中的支持和诊断菜单

通过“支持和诊断”菜单，您可以生成可发送给技术支持以获得故障排除帮助的支持包。

提供以下菜单选项：

- 生成轻量级支持捆绑包

  使您能够生成仅包含 30 天日志和配置数据库记录的轻量级支持包——它不包括性能数据、采集记录文件和服务器堆转储。

- 生成支持包

  允许您在诊断用户的主目录中创建包含诊断信息的完整支持包（7-Zip 文件）。如果您的系统已连接到互联网，您也可以将支持包上传到 NetApp。

  该文件包括由 AutoSupport 消息生成的信息、Unified Manager 数据库的内容、有关 Unified Manager 服务器内部的详细信息以及通常不包含在 AutoSupport 消息或轻量级支持捆绑包中的详细级别日志。

了解有关 **Active IQ Unified Manager** 中其他维护控制台菜单选项的信息

以下菜单选项可用于在 Unified Manager 服务器上执行各种管理任务。

提供以下菜单选项：

- 重置服务器证书

  重新生成 HTTPS 服务器证书。

  您可以通过单击 常规 > **HTTPS** 证书 > 重新生成 **HTTPS** 证书，在 Unified Manager GUI 中重新生成服务器证书。

- 禁用 **SAML** 身份验证

  禁用 SAML 身份验证，以便身份提供程序（IdP）不再为访问 Unified Manager GUI 的用户提供登录身份验证。当 IdP 服务器或 SAML 配置出现问题，导致用户无法访问 Unified Manager GUI 时，通常会使用此控制台选项。

- 外部数据提供商

  提供用于将 Unified Manager 连接到外部数据提供程序的选项。建立连接后，性能数据将发送到外部服务器，以便存储性能专家可以使用第三方软件绘制性能指标图表。此时将显示以下选项：

  - 显示服务器配置--显示外部数据提供程序的当前连接和配置设置。
  - 添加/修改服务器连接--允许您为外部数据提供程序输入新的连接设置，或更改现有设置。
  - 修改服务器配置--允许您为外部数据提供程序输入新的配置设置，或更改现有设置。
  - 删除服务器连接--删除与外部数据提供程序的连接。

    删除连接后，Unified Manager 将失去与外部服务器的连接。

- 备份还原

  有关信息，请参见 "管理备份和还原操作" 下的主题。

- 性能轮询间隔配置

  提供配置 Unified Manager 从群集收集性能统计数据的频率的选项。默认收集间隔为 5 分钟。

  如果发现来自大型集群的收集未按时完成，则可以将此时间间隔更改为 10 或 15 分钟。

- 查看/更改应用程序端口

如果出于安全需要，提供更改 Unified Manager 用于 HTTP 和 HTTPS 协议的默认端口的选项。HTTP 的默认端口为 80，HTTPS 的默认端口为 443。

- 控制对 **MySQL** 端口 **3306** 的访问

  控制主机对默认 MySQL 端口 3306 的访问。出于安全原因，在 Linux、Windows 和 VMware vSphere 系统上全新安装 Unified Manager 期间，通过此端口的访问仅限于本地主机。此选项使您能够在本地主机和远程主机之间切换此端口的可见性，也就是说，如果仅在您的环境中为本地主机启用此端口，您也可以将此端口提供给远程主机。或者，当对所有主机启用时，您可以将此端口的访问限制为仅本地主机。如果以前在远程主机上启用了访问，则在升级场景中保留配置。切换端口可见性后，应检查 Windows 系统上的防火墙设置，如果设置配置为限制对 MySQL 端口 3306 的访问，则应禁用防火墙设置。

- 退出

  退出维护控制台菜单。

在 **Windows** 中更改 **Active IQ Unified Manager** 的维护用户密码

您可以在需要时更改 Unified Manager 维护用户密码。

步骤

1. 在 Unified Manager Web UI 登录页面中，单击 忘记密码。

   此时将显示一个页面，提示输入要重置密码的用户名。

2. 输入用户名并单击*提交*。

   带有重置密码链接的电子邮件将发送到为该用户名定义的电子邮件地址。

3. 单击电子邮件中的*重置密码链接*并定义新密码。
4. 返回到 Web UI 并使用新密码登录到 Unified Manager。

在 **Linux** 系统上更改 **Active IQ Unified Manager umadmin** 密码

出于安全原因，您必须在完成安装过程后立即更改 Unified Manager umadmin 用户的默认密码。如有必要，您可以稍后随时再次更改密码。

开始之前

- Unified Manager 必须安装在 Red Hat Enterprise Linux 系统上。
- 您必须具有安装了 Unified Manager 的 Linux 系统的 root 用户凭据。

步骤

1. 以 root 用户身份登录到运行 Unified Manager 的 Linux 系统。
2. 更改 umadmin 密码：

   ```
   passwd umadmin
   ```

   系统会提示您输入 umadmin 用户的新密码。

更改 **Active IQ Unified Manager** 用于 **HTTP** 和 **HTTPS** 协议的端口

如果出于安全原因需要，可以在安装后更改 Unified Manager 用于 HTTP 和 HTTPS 协议的默认端口。HTTP 的默认端口为 80，HTTPS 的默认端口为 443。

开始之前

您必须拥有已授权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。

> 在使用 Mozilla Firefox 或 Google Chrome 浏览器时，有些端口被认为是不安全的。在为 HTTP 和 HTTPS 流量分配新的端口号之前，请检查您的浏览器。选择不安全的端口可能会导致系统无法访问，这需要您联系客户支持以获得解决方案。

更改端口后，Unified Manager 的实例会自动重新启动，因此请确保这是让系统在短时间内停止运行的好时机。

1. 使用 SSH 作为维护用户登录到 Unified Manager 主机。

   此时将显示 Unified Managermaintenance 控制台提示。

2. 键入标有 **View/Change Application Ports** 的菜单选项编号，然后按 Enter 键。
3. 如果出现提示，请再次输入维护用户密码。
4. 键入 HTTP 和 HTTPS 端口的新端口号，然后按 Enter 键。

   将端口号留空将为协议分配默认端口。

   此时会提示您是否要更改端口并立即重新启动 Unified Manager。

5. 键入 **y** 以更改端口并重新启动 Unified Manager。
6. 退出维护控制台。

此更改后，用户必须在 URL 中包含新端口号才能访问 Unified Manager Web UI，例如 https://host.company.com:1234、https://12.13.14.15:1122 或 https://[2001:db8:0:1]:2123。

向 **Active IQ Unified Manager** 添加网络接口

如果需要分离网络流量，可以添加新的网络接口。

开始之前

您必须已使用 vSphere 将网络接口添加到虚拟设备。

必须打开虚拟设备的电源。

> 如果 Unified Manager 安装在 Red Hat Enterprise Linux 或 Microsoft Windows 上，则无法执行此操作。

步骤

1. 在 vSphere 控制台主菜单中，选择 系统配置 > 重启操作系统。

   重新启动后，维护控制台可以检测到新添加的网络接口。

2. 访问维护控制台。
3. 选择*网络配置* > 启用网络接口。
4. 选择新的网络接口，然后按 **Enter**。

   选择 **eth1**，然后按 **Enter**。

5. 键入 **y** 以启用网络接口。
6. 输入网络设置。

   如果使用静态接口或未检测到 DHCP，系统会提示您输入网络设置。

   输入网络设置后，您将自动返回*网络配置*菜单。

7. 选择*提交更改*。

   必须提交更改才能添加网络接口。

在 **Active IQ Unified Manager** 中重新生成客户端证书

您可以使用维护控制台重新生成 Unified Manager 客户端证书。您的证书有效期延长为五年。

步骤

1. 以维护用户身份登录。
2. 选择*重新生成客户端证书*，然后按*Enter*。
3. 如果系统提示进行身份验证，请输入所需的凭据。
4. 选择 确认重新生成，然后按 **Enter**。
5. 重新生成证书后，重新启动 Unified Manager 服务以应用更改。
6. 要验证更新的证书，请登录到 ONTAP。查看客户端证书状态和有效性状态。

相关信息 "使用 System Manager 管理 ONTAP 证书"

添加磁盘空间

向 **Active IQ Unified Manager** 数据库目录添加磁盘空间

Unified Manager 数据库目录包含从 ONTAP 系统收集的所有运行状况和性能数据。在某些情况下，可能需要增加数据库目录的大小。

例如，如果 Unified Manager 从每个群集都有多个节点的大量群集收集数据，则数据库目录可能会变满。当数据库目录已满 90% 时，您将收到警告事件，当目录已满 95% 时，您将收到严重事件。

目录满 95% 后，不会再从集群中收集其他数据。

向数据目录添加容量所需的步骤不同，具体取决于 Unified Manager 是在 VMware ESXi 服务器上运行、在 Red Hat 服务器上运行还是在 Microsoft Windows 服务器上运行。

在 **Active IQ Unified Manager** 的 **Linux** 主机上向数据目录添加空间

如果您在最初设置 Linux 主机并安装 Unified Manager 时为 `/opt/netapp/data`目录分配的磁盘空间不足以支持 Unified Manager，则可以在安装后通过增加 `/opt/netapp/data`目录上的磁盘空间来添加磁盘空间。

开始之前

您必须具有对安装了 Unified Manager 的 Red Hat Enterprise Linux 计算机的 root 用户访问权限。

建议您在增加数据目录大小之前备份 Unified Manager 数据库。

步骤

1. 以 root 用户身份登录到要添加磁盘空间的 Linux 计算机。
2. 按所示顺序停止 Unified Manager 服务和关联的 MySQL 软件：

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. 创建具有足够磁盘空间的临时备份文件夹（例如 `/backup-data`），以包含当前 `/opt/netapp/data` 目录中的数据。
4. 将现有 `/opt/netapp/data`目录的内容和权限配置复制到备份数据目录：

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

5. 如果启用了 SE Linux：

   a. 获取现有 `/opt/netapp/data`文件夹中文件夹的 SE Linux 类型：

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      系统将返回类似于以下内容的确认消息：

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. 运行 chcon 命令为备份目录设置 SE Linux 类型：

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. 删除 `/opt/netapp/data`目录的内容：

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. 通过 LVM 命令或添加额外磁盘，将 `/opt/netapp/data`目录的大小扩展到至少 150 GB。

   如果您从磁盘创建了 `/opt/netapp/data`，则不应尝试将 `/opt/netapp/data`作为 `NFS` 或 `CIFS` 共享进行挂载。因为在这种情况下，如果您尝试扩展磁盘空间，某些 `LVM` 命令（

如 `resize`和 `extend`）可能无法按预期工作。

8. 确认 `/opt/netapp/data`目录所有者（mysql）和组（root）未更改：

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

   系统将返回类似于以下内容的确认消息：

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

9. 如果启用了 SE Linux，请确认 `/opt/netapp/data` 目录的上下文仍然设置为 mysqld_db_t：

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

      系统将返回类似于以下内容的确认消息：

   ```
   -rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
   /opt/netapp/data/abc
   ```

10. 删除文件 abc，以免这个多余的文件在将来引发数据库错误。
11. 将 backup-data 中的内容复制回扩展的 `/opt/netapp/data`目录：

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

12. 如果启用了 SE Linux，请运行以下命令：

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

13. 启动 MySQL 服务：

    ```
    systemctl start mysqld
    ```

14. MySQL 服务启动后，按所示顺序启动 ocie 和 ocieau 服务：

    ```
    systemctl start ocie ocieau
    ```

15. 所有服务启动后，删除备份文件夹 `/backup-data`：

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

在 **Active IQ Unified Manager** 中向 **VMware** 虚拟机上的数据磁盘添加空间

如果需要增加 Unified Manager 数据库的数据磁盘上的空间量，可以在安装后通过使用 Unified Manager 维护控制台增加磁盘空间来添加容量。

开始之前

- 您必须能够访问 vSphere 客户端。
- 虚拟机必须没有本地存储的快照。
- 您必须具有维护用户凭据。

建议您在增加虚拟磁盘大小之前备份虚拟机。

步骤

1. 在 vSphere 客户端中，选择 Unified Manager 虚拟机，然后向数据 `disk 3`添加更多磁盘容量。有关详细信息，请参阅 VMware 文档。

   在某些罕见情况下，Unified Manager 部署使用 “Hard Disk 2” 作为数据磁盘，而不是 “Hard Disk 3”。如果在您的部署中发生此情况，请增加较大磁盘的空间。数据磁盘的空间将始终大于另一个磁盘。

2. 在 vSphere 客户端中，选择 Unified Manager 虚拟机，然后选择*控制台*选项卡。
3. 在控制台窗口中单击，然后使用您的用户名和密码登录到维护控制台。
4. 在主菜单中，输入*系统配置*选项的编号。
5. 在系统配置菜单中，输入*增加数据磁盘大小*选项的数字。

在 **Active IQ Unified Manager** 中向 **Windows** 服务器上的逻辑驱动器添加空间

如果需要增加 Unified Manager 数据库的磁盘空间量，可以向安装 Unified Manager 的逻辑驱动器添加容量。

开始之前

您必须具有 Windows 管理员权限。

我们建议您在添加磁盘空间之前备份 Unified Manager 数据库。

步骤

1. 以管理员身份登录到要添加磁盘空间的 Windows 服务器。
2. 请按照要添加更多空间的方法对应的步骤操作：

选项	问题描述
在物理服务器上，向安装有 Unified Manager 服务器的逻辑驱动器添加容量。	按照 Microsoft 主题中的步骤操作： "扩展基本卷"
在物理服务器上，添加硬盘驱动器。	按照 Microsoft 主题中的步骤操作： "添加硬盘驱动器"
在虚拟机上，增加磁盘分区的大小。	按照 VMware 主题中的步骤操作： "增加磁盘分区的大小"

管理用户访问

添加用户

在 **Active IQ Unified Manager** 中添加用户

您可以使用“用户”页面添加本地用户或数据库用户。您还可以添加属于身份验证服务器的远程用户或组。您可以为这些用户分配角色，并且根据角色的权限，用户可以使用 Unified Manager 管理存储对象和数据，或查看数据库中的数据。

开始之前

- 您必须具有应用程序管理员角色。
- 要添加远程用户或组，您必须启用远程身份验证并配置身份验证服务器。
- 如果您计划配置 SAML 身份验证，以便身份提供程序（IdP）对访问图形界面的用户进行身份验证，请确保将这些用户定义为 “remote” 用户。

  启用 SAML 身份验证时，不允许类型为“`local`”或“`maintenance`”的用户访问 UI。

如果从 Windows Active Directory 添加组，则所有直接成员和嵌套子组都可以向 Unified Manager 进行身份验证，除非嵌套子组被禁用。如果从 OpenLDAP 或其他身份验证服务添加组，则只有该组的直接成员才能向 Unified Manager 进行身份验证。

步骤

1. 在左侧导航窗格中，单击 常规 > 用户。
2. 在“用户”页面上，单击*添加*。
3. 在“添加用户”对话框中，选择要添加的用户类型，然后输入所需信息。

   输入所需的用户信息时，您必须指定该用户唯一的电子邮件地址。您必须避免指定由多个用户共享的电子邮件地址。

4. 单击 **Add**。

在 **Active IQ Unified Manager** 中创建数据库用户

若要支持 Workflow Automation 和 Unified Manager 之间的连接或访问数据库视图，必须首先在 Unified Manager Web UI 中创建具有“集成架构”或“报告架构”角色的数据库用户。

开始之前

您必须具有应用程序管理员角色。

数据库用户提供与 Workflow Automation 的集成以及对特定于报表的数据库视图的访问。数据库用户无权访问 Unified Manager Web UI 或维护控制台，并且无法执行 API 调用。

步骤

1. 在左侧导航窗格中，单击 常规 > 用户。
2. 在用户页面中，单击*添加*。

3. 在添加用户对话框中，在*类型*下拉列表中选择*数据库用户*。
4. 键入此数据库用户的名称和密码。
5. 在*角色*下拉列表中，选择相应的角色。

如果您是……	选择此角色
将 Unified Manager 与 Workflow Automation 连接	集成架构
访问报告和其他数据库视图	报告架构

6. 单击 **Add**。

在 **Active IQ Unified Manager** 中编辑用户设置

您可以编辑为每个用户指定的用户设置（例如电子邮件地址和角色）。例如，您可能希望更改存储操作员用户的角色，并将存储管理员权限分配给该用户。

开始之前

您必须具有应用程序管理员角色。

当您修改分配给用户的角色时，会在发生以下任一操作时应用更改：

- 用户注销并重新登录到 Unified Manager。
- 已达到 24 小时的会话超时。

步骤

1. 在左侧导航窗格中，单击 常规 > 用户。
2. 在用户页面中，选择要编辑设置的用户，然后单击*编辑*。
3. 在编辑用户对话框中，编辑为此用户指定的相应设置。
4. 单击 **Save**。

在 **Active IQ Unified Manager** 中查看用户

您可以使用“用户”页面查看使用 Unified Manager 管理存储对象和数据的用户列表。您可以查看有关用户的详细信息，例如用户名、用户类型、电子邮件地址以及分配给用户的角色。

开始之前

您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击 常规 > 用户。

删除 **Active IQ Unified Manager** 中的用户或组

您可以从管理服务器数据库中删除一个或多个用户，以防止特定用户访问 Unified

Manager。您还可以删除组，以便组中的所有用户都无法再访问管理服务器。

开始之前

- 删除远程组时，必须重新分配已分配给远程组用户的事件。

  如果要删除本地用户或远程用户，则分配给这些用户的事件将自动取消分配。

- 您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击 常规 > 用户。
2. 在“用户”页面中，选择要删除的用户或组，然后单击 删除。
3. 单击 是 确认删除。

了解 **Active IQ Unified Manager** 中基于角色的访问控制

RBAC（基于角色的访问控制）提供了控制谁有权访问 Active IQ Unified Manager 服务器中的各种功能和资源的功能。RBAC 使管理员能够通过定义角色来管理用户组。如果需要将特定功能的访问权限限制为选定管理员，则必须为其设置管理员帐户。如果要限制管理员可以查看的信息及其可以执行的操作，则必须将角色应用于创建的管理员帐户。

管理服务器使用 RBAC 进行用户登录和角色权限管理。如果您没有更改管理服务器的管理用户访问默认设置，则无需登录即可查看它们。

当您启动需要特定权限的操作时，管理服务器会提示您登录。例如，要创建管理员帐户，必须使用应用程序管理员帐户访问权限登录。

了解 **Active IQ Unified Manager** 中的用户类型

用户类型指定用户持有的帐户类型，包括远程用户、远程组、本地用户、数据库用户和维护用户。每种类型都有自己的角色，由具有管理员角色的用户分配。

Unified Manager 用户类型如下：

- 维护用户

  在 Unified Manager 的初始配置期间创建。然后，维护用户创建其他用户并分配角色。维护用户也是唯一有权访问维护控制台的用户。在 Red Hat Enterprise Linux 系统上安装 Unified Manager 时，维护用户将被赋予用户名 “umadmin.”

- 本地用户

  访问 Unified Manager UI 并根据维护用户或具有应用程序管理员角色的用户赋予的角色执行功能。

- 远程组

  使用存储在身份验证服务器上的凭据访问 Unified Manager UI 的一组用户。此帐户的名称应与存储在身份验证服务器上的组的名称相匹配。远程组中的所有用户都可以使用其个人用户凭据访问 Unified Manager UI。远程组可以根据其分配的角色执行功能。

- 远程用户

  使用存储在身份验证服务器上的凭据访问 Unified Manager UI。远程用户根据维护用户或具有应用程序管理员角色的用户赋予的角色执行功能。

- 数据库用户

  对 Unified Manager 数据库中的数据具有只读访问权限，无权访问 Unified Manager Web 界面或维护控制台，并且无法执行 API 调用。

了解 **Active IQ Unified Manager** 中的用户角色

维护用户或应用程序管理员为每个用户分配一个角色。每个角色都包含某些特权。您可以在 Unified Manager 中执行的活动范围取决于分配给您的角色以及该角色包含的权限。

Unified Manager 包括以下预定义的用户角色：

- 操作员

  查看存储系统信息以及 Unified Manager 收集的其他数据，包括历史记录和容量趋势。此角色使存储操作员能够查看、分配、确认、解决事件并为事件添加备注。

- 存储管理员

  在 Unified Manager 中配置存储管理操作。此角色使存储管理员能够配置阈值并创建警报和其他特定于存储管理的选项和策略。

- 应用程序管理员

  配置与存储管理无关的设置。此角色允许管理用户、安全证书、数据库访问和管理选项，包括身份验证、SMTP、网络和 AutoSupport。

  在 Linux 系统上安装 Unified Manager 时，具有应用程序管理员角色的初始用户将自动命名为“umadmin”。

- 集成架构

  此角色允许对 Unified Manager 数据库视图进行只读访问，以便将 Unified Manager 与 OnCommand Workflow Automation （WFA） 集成。

- 报告架构

  此角色可直接从 Unified Manager 数据库以只读方式访问报告和其他数据库视图。可查看的数据库包括：

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt

- opm
- scalemonitor

了解 **Active IQ Unified Manager** 中的用户角色和功能

根据您分配的用户角色，您可以确定可以在 Unified Manager 中执行哪些操作。

下表显示了每个用户角色可以执行的功能：

功能	运算符	存储管理员	应用程序管理员	集成架构	报告架构
查看存储系统信息	•	•	•	•	•
查看其他数据，例如历史记录和容量趋势	•	•	•	•	•
查看、分配和解决事件	•	•	•		
查看存储服务对象，例如 SVM 关联和资源池	•	•	•		
查看阈值策略	•	•	•		
管理存储服务对象，例如 SVM 关联和资源池		•	•		
定义警报		•	•		
管理存储管理选项		•	•		
管理存储管理策略		•	•		
管理用户			•		
管理管理选项			•		
定义阈值策略			•		
管理数据库访问			•		
管理与 WFA 的集成并提供对数据库视图的访问				•	
安排并保存报告		•	•		
从管理操作执行“Fix It” 操作		•	•		
提供对数据库视图的只读访问权限					•

管理 SAML 身份验证设置

在 Active IQ Unified Manager 中启用 SAML 身份验证

配置远程身份验证设置后，您可以启用安全断言标记语言（SAML）身份验证，以便远程用户在访问 Unified Manager Web UI 之前由安全身份提供程序（IdP）进行身份验证。

请注意，只有远程用户才能在启用 SAML 身份验证后访问 Unified Manager 图形用户界面。本地用户和维护用户将无法访问 UI。此配置不会影响访问维护控制台的用户。

在 Active IQ Unified Manager 中使用身份提供程序

在将 Unified Manager 配置为使用身份提供程序（IdP）为所有远程用户执行 SAML 身份验证时，您需要了解一些必需的配置设置，以便成功连接到 Unified Manager。

必须在 IdP 服务器中输入 Unified Manager URI 和元数据。您可以从 Unified ManagerSAML 身份验证页面复制此信息。在安全断言标记语言（SAML）标准中，Unified Manager 被视为服务提供程序（SP）。

支持的加密标准

- 高级加密标准（AES）：AES-128 和 AES-256
- 安全哈希算法（SHA）：SHA-1 和 SHA-256

已验证的身份提供程序

- Shibboleth
- Active Directory 联合身份验证服务（ADFS）

ADFS 配置要求

- 必须按以下顺序定义三个声明规则，这些规则是 Unified Manager 解析此依赖方信任项的 ADFS SAML 响应所必需的。

声明规则	值
SAM-account-name	名称 ID
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
令牌组 — 未限定名称	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- 您必须将身份验证方法设置为“表单身份验证”，否则用户在注销 Unified Manager 时可能会收到错误。按照以下步骤操作：
  a. 打开 ADFS 管理控制台。
  b. 单击左侧树视图上的身份验证策略文件夹。
  c. 在右侧的“操作”下，单击“编辑全局主要身份验证策略”。
  d. 将 Intranet 身份验证方法设置为“`Forms Authentication`”，而不是默认的“`Windows Authentication`”。

- 在某些情况下，当 Unified Manager 安全证书经过 CA 签名时，通过 IdP 登录会被拒绝。有两种解决方法可以解决此问题：
  - 按照链接中标识的说明，在 ADFS 服务器上禁用链式 CA 证书关联依赖方的吊销检查：

    "禁用每个依赖方信任的吊销检查"

  - 请让 CA 服务器驻留在 ADFS 服务器内，以便对 Unified Manager 服务器证书请求进行签名。

其他配置要求

- Unified Manager 时钟偏差设置为 5 分钟，因此 IdP 服务器和 Unified Manager 服务器之间的时间差不能超过 5 分钟，否则身份验证将失败。

在 **Active IQ Unified Manager** 中启用 **SAML** 身份验证

您可以启用安全断言标记语言（SAML）身份验证，以便远程用户在访问 Unified Manager Web UI 之前由安全身份提供程序（IdP）进行身份验证。

开始之前

- 您必须已配置远程身份验证并验证其成功。
- 您必须至少创建了一个具有应用程序管理员角色的远程用户或远程组。
- Unified Manager 必须支持身份提供程序（IdP），并且必须对其进行配置。
- 您必须具有 IdP URL 和元数据。
- 您必须能够访问 IdP 服务器。

从 Unified Manager 启用 SAML 身份验证后，在使用 Unified Manager 服务器主机信息配置 IdP 之前，用户无法访问图形用户界面。因此，在开始配置过程之前，您必须准备好完成连接的两个部分。可以在配置 Unified Manager 之前或之后配置 IdP。

启用 SAML 身份验证后，只有远程用户才能访问 Unified Manager 图形用户界面。本地用户和维护用户将无法访问 UI。此配置不会影响访问维护控制台、Unified Manager 命令或 ZAPI 的用户。

完成此页面上的 SAML 配置后，Unified Manager 将自动重新启动。

步骤

1. 在左侧导航窗格中，单击*常规* > **SAML** 身份验证。
2. 选中 启用 **SAML** 身份验证 复选框。

   将显示配置 IdP 连接所需的字段。

3. 请输入将 Unified Manager 服务器连接到 IdP 服务器所需的 IdP URI 和 IdP 元数据。

   如果可以直接从 Unified Manager 服务器访问 IdP 服务器，您可以在输入 IdP URI 后单击 获取 **IdP** 元数据 按钮，以自动填充 IdP 元数据字段。

4. 复制 Unified Manager 主机元数据 URI，或将主机元数据保存到 XML 文本文件。

您此时可以使用此信息配置 IdP 服务器。

5. 单击 **Save**。

   此时将显示一个消息框，以确认您要完成配置并重新启动 Unified Manager。

6. 单击 确认并注销，Unified Manager 将重新启动。

下次授权远程用户尝试访问 Unified Manager 图形界面时，他们将在 IdP 登录页面而不是 Unified Manager 登录页面中输入其凭据。

如果尚未完成，请访问您的 IdP 并输入 Unified Manager 服务器 URI 和元数据以完成配置。

> 将 ADFS 用作身份提供程序时，Unified Manager GUI 不会遵守 ADFS 超时，并且将继续工作，直到达到 Unified Manager 会话超时。您可以通过单击 常规 > 功能设置 > 非活动超时 来更改 GUI 会话超时。

在 **Active IQ Unified Manager** 中更改 **SAML** 身份验证标识提供程序

您可以更改 Unified Manager 用来验证远程用户的身份提供程序（IdP）。

开始之前

- 您必须具有 IdP URL 和元数据。
- 您必须能够访问 IdP。

可以在配置 Unified Manager 之前或之后配置新的 IdP。

步骤

1. 在左侧导航窗格中，单击*常规* > **SAML** 身份验证。
2. 请输入将 Unified Manager 服务器连接到 IdP 所需的新 IdP URI 和 IdP 元数据。

   如果可以直接从 Unified Manager 服务器访问 IdP，您可以在输入 IdP URL 后单击 获取 **IdP** 元数据 按钮，以自动填充 IdP 元数据字段。

3. 复制 Unified Manager 元数据 URI，或将元数据保存到 XML 文本文件。
4. 单击*保存配置*。

   此时将显示一个消息框，以确认您要更改配置。

5. 单击 **OK**。

请访问新的 IdP 并输入 Unified Manager 服务器 URI 和元数据以完成配置。

下次授权远程用户尝试访问 Unified Manager 图形界面时，他们将在新的 IdP 登录页面而不是旧的 IdP 登录页面中输入其凭据。

在 **Active IQ Unified Manager** 安全证书更改后更新 **SAML** 身份验证设置

对 Unified Manager 服务器上安装的 HTTPS 安全证书进行任何更改都需要更新 SAML 身

份验证配置设置。如果重命名主机系统、为主机系统分配新的 IP 地址或手动更改系统的安全证书，则会更新证书。

更改安全证书并重新启动 Unified Manager 服务器后，SAML 身份验证将无法运行，用户将无法访问 Unified Manager 图形界面。必须在 IdP 服务器和 Unified Manager 服务器上更新 SAML 身份验证设置，才能重新启用对用户界面的访问。

步骤

1. 登录维护控制台。
2. 在*主菜单*中，输入*禁用 SAML 身份验证*选项的数字。

   系统将显示一条消息，以确认您要禁用 SAML 身份验证并重新启动 Unified Manager。
3. 使用更新的 FQDN 或 IP 地址启动 Unified Manager 用户界面，在浏览器中接受更新的服务器证书，然后使用维护用户凭据登录。
4. 在 设置/身份验证 页面中，选择 **SAML** 身份验证 选项卡并配置 IdP 连接。
5. 复制 Unified Manager 主机元数据 URI，或将主机元数据保存到 XML 文本文件。
6. 单击 **Save**。

   此时将显示一个消息框，以确认您要完成配置并重新启动 Unified Manager。
7. 单击 确认并注销，Unified Manager 将重新启动。
8. 请访问您的 IdP 服务器并输入 Unified Manager 服务器 URI 和元数据以完成配置。

身份提供程序	配置步骤
ADFS	a. 删除 ADFS 管理 GUI 中的现有依赖方信任条目。 b. 使用更新后的 Unified Manager 服务器中的 `saml_sp_metadata.xml`添加新的依赖方信任项。 c. 定义 Unified Manager 解析此依赖方信任条目的 ADFS SAML 响应所需的三个声明规则。 d. 重新启动 ADFS Windows 服务。
Shibboleth	a. 将 Unified Manager 服务器的新 FQDN 更新到 `attribute-filter.xml`和 `relying-party.xml`文件中。 b. 重新启动 Apache Tomcat Web 服务器，并等待端口 8005 联机。

9. 登录到 Unified Manager，并通过 IdP 验证 SAML 身份验证是否按预期工作。

在 **Active IQ Unified Manager** 中禁用 **SAML** 身份验证

如果要在远程用户登录到 Unified Manager Web UI 之前停止通过安全身份提供程序（IdP）对其进行身份验证，则可以禁用 SAML 身份验证。禁用 SAML 身份验证时，已配置的目

录服务提供程序（如 Active Directory 或 LDAP）将执行登录身份验证。

禁用 SAML 身份验证后，除了已配置的远程用户外，本地用户和维护用户还可以访问图形用户界面。

如果您无权访问图形用户界面，也可以使用 Unified Manager 维护控制台禁用 SAML 身份验证。

禁用 SAML 身份验证后，将自动重新启动 Unified Manager。

步骤

1. 在左侧导航窗格中，单击*常规* > **SAML** 身份验证。
2. 取消选中 启用 **SAML** 身份验证 复选框。
3. 单击 **Save**。

   此时将显示一个消息框，以确认您要完成配置并重新启动 Unified Manager。

4. 单击 确认并注销，Unified Manager 将重新启动。

下次远程用户尝试访问 Unified Manager 图形界面时，他们将在 Unified Manager 登录页面而不是 IdP 登录页面中输入其凭据。

请访问您的 IdP 并删除 Unified Manager 服务器 URI 和元数据。

从 **Active IQ Unified Manager** 维护控制台禁用 **SAML** 身份验证

当无法访问 Unified Manager GUI 时，您可能需要从维护控制台禁用 SAML 身份验证。这可能发生在配置错误或 IdP 不可访问的情况下。

开始之前

您必须能够以维护用户的身份访问维护控制台。

禁用 SAML 身份验证时，已配置的目录服务提供程序（如 Active Directory 或 LDAP）将执行登录身份验证。除了已配置的远程用户外，本地用户和维护用户也将能够访问图形用户界面。

您还可以从 UI 中的“设置/身份验证”页面禁用 SAML 身份验证。

禁用 SAML 身份验证后，将自动重新启动 Unified Manager。

步骤

1. 登录维护控制台。
2. 在*主菜单*中，输入*禁用 SAML 身份验证*选项的数字。

   系统将显示一条消息，以确认您要禁用 SAML 身份验证并重新启动 Unified Manager。

3. 键入 **y**，然后按 Enter，Unified Manager 将重新启动。

下次远程用户尝试访问 Unified Manager 图形界面时，他们将在 Unified Manager 登录页面而不是 IdP 登录页面中输入其凭据。

如果需要，请访问您的 IdP 并删除 Unified Manager 服务器 URL 和元数据。

使用 **Active IQ Unified Manager** 中的 **SAML** 身份验证页面

您可以使用 SAML 身份验证页面将 Unified Manager 配置为使用 SAML 通过安全身份提供程序（IdP）对远程用户进行身份验证，然后他们才能登录到 Unified Manager web UI。

- 您必须具有应用程序管理员角色才能创建或修改 SAML 配置。
- 您必须事先配置远程身份验证。
- 您必须事先至少配置一个远程用户或远程组。

配置远程身份验证和远程用户后，您可以选中启用 SAML 身份验证复选框，以启用使用安全身份提供程序的身份验证。

- **IdP URI**

  从 Unified Manager 服务器访问 IdP 的 URI。以下列出了示例 URI。

  ADFS 的示例 URI：

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

  Shibboleth 的示例 URI：

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

- **IdP** 元数据

  XML 格式的 IdP 元数据。

  如果可以从 Unified Manager 服务器访问 IdP URL，则可以单击 获取 **IdP** 元数据 按钮以填充此字段。

- 主机系统（**FQDN**）

  安装期间定义的 Unified Manager 主机系统的 FQDN。如有必要，您可以更改此值。

- 主机 **URI**

  用于从 IdP 访问 Unified Manager 主机系统的 URI。

- 主机元数据

  XML 格式的主机系统元数据。

管理身份验证

在 **Active IQ Unified Manager** 中编辑身份验证服务器

您可以更改 Unified Manager 服务器用于与身份验证服务器通信的端口。

开始之前

您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 选中 **Disable Nested Group Lookup**（禁用嵌套组查找）框。
3. 在*身份验证服务器*区域中，选择要编辑的身份验证服务器，然后单击*编辑*。
4. 在*编辑身份验证服务器*对话框中，编辑端口详细信息。
5. 单击 **Save**。

删除 **Active IQ Unified Manager** 中的身份验证服务器

如果要阻止 Unified Manager 服务器与身份验证服务器通信，则可以删除身份验证服务器。例如，如果要更改与管理服务器通信的身份验证服务器，则可以删除身份验证服务器并添加新的身份验证服务器。

开始之前

您必须具有应用程序管理员角色。

删除身份验证服务器时，身份验证服务器的远程用户或组将无法再访问 Unified Manager。

步骤

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 选择要删除的一个或多个身份验证服务器，然后单击*删除*。
3. 单击 是 确认删除请求。

   如果启用了*使用安全连接*选项，则与身份验证服务器关联的证书将与身份验证服务器一起删除。

在 **Active IQ Unified Manager** 中使用 **Active Directory** 或 **OpenLDAP** 进行身份验证

您可以在管理服务器上启用远程身份验证，并将管理服务器配置为与您的身份验证服务器进行通信，以便身份验证服务器内的用户可以访问 Unified Manager。

可以使用以下预定义的身份验证服务之一，也可以指定自己的身份验证服务：

- Microsoft Active Directory

  您不能使用 Microsoft Lightweight Directory Services。

- OpenLDAP

您可以选择所需的身份验证服务并添加适当的身份验证服务器，以使身份验证服务器中的远程用户能够访问

Unified Manager。远程用户或组的凭据由身份验证服务器维护。管理服务器使用轻型目录访问协议（LDAP）对配置的身份验证服务器中的远程用户进行身份验证。

对于在 Unified Manager 中创建的本地用户，管理服务器维护其自己的用户名和密码数据库。管理服务器执行身份验证，不使用 Active Directory 或 OpenLDAP 进行身份验证。

审核日志记录

了解 **Active IQ Unified Manager** 中的审核日志

您可以使用审核日志来检测审核日志是否已受损。用户执行的所有活动都将受到监控并记录在审核日志中。审核针对 Active IQ Unified Manager 的所有用户界面和公开的 API 功能执行。

您可以使用*审核日志：文件视图*查看和访问 Active IQ Unified Manager 中可用的所有审核日志文件。审核日志：文件视图中的文件将根据其创建日期列出。此视图显示从安装或升级到目前为止在系统中捕获的所有审核日志的信息。每当您在 Unified Manager 中执行操作时，信息都会更新并在日志中可用。每个日志文件的状态是使用“File Integrity Status”属性捕获的，该属性受到主动监控，以检测日志文件是否被篡改或删除。当审核日志在系统中可用时，审核日志可以具有以下状态之一：

州/省	问题描述
处于活动状态	当前正在记录日志的文件。
正常	非活动、压缩并存储在系统中的文件。
已篡改	已被手动编辑该文件的用户破坏的文件。
MANUAL_DELETE	已被授权用户删除的文件。
ROLLOVER_DELETE	由于根据滚动配置策略滚动而被删除的文件。
UNEXPECTED_DELETE	由于未知原因而被删除的文件。

审核日志页面包含以下命令按钮：

- 配置
- 删除
- 下载

DELETE 按钮使您能够删除审核日志视图中列出的任何审核日志。您可以删除审核日志，并可选择提供删除文件的原因，这有助于将来确定有效的删除。REASON 列列出原因以及执行删除操作的用户的名称。

删除日志文件将导致从系统中删除文件，但不会删除 DB 表中的条目。

您可以使用审核日志部分中的 下载 按钮从 Active IQ Unified Manager 下载审核日志并导出审核日志文件。标记为“NORMAL”或“TAMPERED”的文件将以压缩 `.gzip`格式下载。

审核日志文件定期存档并保存到数据库中以供参考。在存档之前，审核日志经过数字签名，以维护安全性和完整性。

生成完整的 AutoSupport 捆绑包时，支持捆绑包将包含已归档和活动的审核日志文件。但是，当生成轻型支持捆绑包时，它仅包含活动的审核日志。不包含已归档的审核日志。

配置 **Active IQ Unified Manager** 审核日志

您可以使用审核日志部分中的*配置*按钮来配置审核日志文件的滚动策略，并启用审核日志的远程日志记录。

您可以根据要在系统中存储的数据量和频率，设置 **MAX FILE SIZE** 和 **AUDIT LOG RETENTION DAYS** 的值。**TOTAL AUDIT LOG SIZE** 字段中的值是系统中存在的审核日志数据的总大小。滚动策略由 **AUDIT LOG RETENTION DAYS**、**MAX FILE SIZE** 和 **TOTAL AUDIT LOG SIZE** 字段中的值决定。当审核日志备份的大小达到 **TOTAL AUDIT LOG SIZE** 中配置的值时，将删除最先归档的文件。这意味着最旧的文件将被删除。但该文件条目在数据库中仍然可用，并被标记为“`Rollover Delete`”。**AUDIT LOG RETENTION DAYS** 值用于指定保留审核日志文件的天数。任何早于此字段中设置值的文件都将被滚动。

步骤

1. 单击*审核日志* > > 配置。
2. 在*最大文件大小*、*总审计日志大小*和*审计日志保留天数*中输入值。

   要启用远程日志记录，请选择*启用远程日志记录*。

在 **Active IQ Unified Manager** 中启用审计日志的远程日志记录

您可以在“配置审核日志”对话框中选中 启用远程日志记录 复选框以启用远程审核日志记录。您可以使用此功能将审核日志传输到远程 Syslog 服务器。这使您能够在受到空间限制时管理审核日志。

审核日志的远程日志记录提供了防篡改备份，以防 Active IQ Unified Manager 服务器上的审核日志文件被篡改。

步骤

1. 在*配置审计日志*对话框中，选中*启用远程日志记录*复选框。

   此时将显示用于配置远程日志记录的其他字段。

2. 输入要连接到的远程服务器的*主机名*和*端口*。
3. 在*服务器 CA 证书*字段中，单击*浏览*以选择目标服务器的公共证书。

   证书应以 `.pem`格式上传。此证书应从目标 `Syslog` 服务器获取且不应过期。证书应包含选定的 “`hostname`” 作为 `SubjectAltName` （SAN）属性的一部分。

4. 输入以下字段的值：**CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

   这些字段的值应以毫秒为单位。

5. 在 格式 和 协议 字段中选择所需的 Syslog 格式和 TLS 协议版本。
6. 如果目标 Syslog 服务器需要基于证书的身份验证，请选中*启用客户端身份验证*复选框。

   在保存审核日志配置之前，您需要下载客户端身份验证证书并将其上传到 Syslog 服务器，否则连接将失败。根据 Syslog 服务器的类型，可能需要创建客户端身份验证证书的哈希。

   示例：syslog-ng 需要使用命令 `openssl x509 -noout -hash -in cert.pem` 创建证书的 <hash>，然后您应将客户端身份验证证书符号链接到以 <hash> .0 命名的文件。

7. 单击 保存 以配置与服务器的连接并启用远程日志记录。

   您将被重定向至“审核日志”页面。

   *连接超时*值可能会影响配置。如果配置的响应时间长于定义的值，则可能由于连接错误而导致配置失败。要建立成功的连接，请增加*连接超时*值，然后重试配置。

使用 **Active IQ Unified Manager** 中的远程身份验证页面

您可以使用“远程身份验证”页面配置 Unified Manager 与您的身份验证服务器进行通信，以对尝试登录到 Unified Manager Web UI 的远程用户进行身份验证。

您必须具有应用程序管理员或存储管理员角色。

选中启用远程身份验证复选框后，可以使用身份验证服务器启用远程身份验证。

- 身份验证服务

  使您能够配置管理服务器，以便在目录服务提供程序（如 Active Directory、OpenLDAP）中对用户进行身份验证，或者指定您自己的身份验证机制。仅当启用了远程身份验证时，才能指定身份验证服务。

  - **Active Directory**
    - 管理员名称

      指定身份验证服务器的管理员名称。

    - 密码

      指定访问身份验证服务器的密码。

    - 基本可分辨名称

      指定远程用户在身份验证服务器中的位置。例如，如果身份验证服务器的域名是 ou@domain.com，则基本可分辨名称是 **cn=ou,dc=domain,dc=com**。

    - 禁用嵌套组查找

      指定是启用还是禁用嵌套组查找选项。默认情况下，此选项处于禁用状态。如果使用 Active Directory，则可以通过禁用对嵌套组的支持来加快身份验证速度。

    - 使用安全连接

      指定用于与身份验证服务器通信的身份验证服务。

  - **OpenLDAP**
    - 绑定可分辨名称

      指定与基本可分辨名称一起使用的绑定可分辨名称，以在身份验证服务器中查找远程用户。

    - 绑定密码

指定访问身份验证服务器的密码。

- 基本可分辨名称

  指定远程用户在身份验证服务器中的位置。例如，如果身份验证服务器的域名是 ou@domain.com，则基本可分辨名称是 **cn=ou,dc=domain,dc=com**。

- 使用安全连接

  指定使用安全 LDAP 与 LDAP 身份验证服务器进行通信。

◦ 其他

- 绑定可分辨名称

  指定与基本可分辨名称一起使用的 bind 可分辨名称，以在已配置的身份验证服务器中查找远程用户。

- 绑定密码

  指定访问身份验证服务器的密码。

- 基本可分辨名称

  指定远程用户在身份验证服务器中的位置。例如，如果身份验证服务器的域名是 ou@domain.com，则基本可分辨名称是 **cn=ou,dc=domain,dc=com**。

- 协议版本

  指定身份验证服务器支持的轻型目录访问协议（LDAP）版本。您可以指定是否必须自动检测协议版本，或将版本设置为 2 或 3。

- 用户名属性

  指定身份验证服务器中包含要由管理服务器进行身份验证的用户登录名的属性的名称。

- 组成员资格属性

  指定一个值，该值基于用户身份验证服务器中指定的属性和值将管理服务器组成员身份分配给远程用户。

- UGID

  如果远程用户作为 GroupOfUniqueNames 对象的成员包含在身份验证服务器中，则此选项使您能够根据该 GroupOfUniqueNames 对象中的指定属性将管理服务器组成员身份分配给远程用户。

- 禁用嵌套组查找

  指定是启用还是禁用嵌套组查找选项。默认情况下，此选项处于禁用状态。如果使用 Active Directory，则可以通过禁用对嵌套组的支持来加快身份验证速度。

- 成员

指定身份验证服务器用于存储有关组个别成员的信息的属性名称。

- 用户对象类

  指定远程身份验证服务器中用户的对象类。

- 组对象类

  指定远程身份验证服务器中所有组的对象类。

  > 为 *Member*、*User Object Class* 和 *Group Object Class* 属性输入的值应与 Active Directory、OpenLDAP 和 LDAP 配置中添加的值相同。否则，身份验证可能会失败。

- 使用安全连接

  指定用于与身份验证服务器通信的身份验证服务。

> 如果要修改身份验证服务，请确保删除所有现有的身份验证服务器并添加新的身份验证服务器。

身份验证服务器区域

身份验证服务器区域显示管理服务器与之通信以查找和对远程用户进行身份验证的身份验证服务器。远程用户或组的凭据由身份验证服务器维护。

- 命令按钮

  允许您添加、编辑或删除身份验证服务器。

  - 添加

    允许您添加身份验证服务器。

  如果要添加的身份验证服务器是高可用性对的一部分（使用相同的数据库），则还可以添加伙伴身份验证服务器。这使管理服务器能够在其中一个身份验证服务器无法访问时与伙伴通信。

  - 编辑

    允许您编辑所选身份验证服务器的设置。

  - 删除

    删除选定的身份验证服务器。

- 名称或 **IP** 地址

  显示用于对管理服务器上的用户进行身份验证的身份验证服务器的主机名或 IP 地址。

- 端口

  显示身份验证服务器的端口号。

- 测试身份验证

此按钮通过对远程用户或组进行身份验证来验证身份验证服务器的配置。

在测试期间，如果仅指定用户名，则管理服务器会在身份验证服务器中搜索远程用户，但不会对用户进行身份验证。如果同时指定用户名和密码，则管理服务器将搜索远程用户并对其进行身份验证。

如果禁用远程身份验证，则无法测试身份验证。

管理安全证书

在 **Active IQ Unified Manager** 中查看 **HTTPS** 安全证书

您可以将 HTTPS 证书详细信息与浏览器中检索的证书进行比较，以确保浏览器与 Unified Manager 的加密连接不会被截获。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

查看证书使您能够验证重新生成的证书的内容，或查看可以从中访问 Unified Manager 的使用者备用名称（SAN）。

步骤

1. 在左侧导航窗格中，单击 常规 > **HTTPS** 证书。

   此时 HTTPS 证书将显示在页面顶部。

如果您需要查看比 HTTPS 证书页面上显示的更详细的安全证书信息，则可以在浏览器中查看连接证书。

在 **Active IQ Unified Manager** 中下载 **HTTPS** 证书签名请求

您可以下载当前 HTTPS 安全证书的证书签名请求，以便将该文件提供给证书颁发机构进行签名。CA 签名证书有助于防止中间人攻击，并提供比自签名证书更好的安全保护。

开始之前

您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击 常规 > **HTTPS** 证书。
2. 单击*下载 HTTPS 证书签名请求*。
3. 保存 `<hostname>.csr`文件。

您可以将文件提供给证书颁发机构以签名，然后安装签名证书。

在 **Active IQ Unified Manager** 中安装 **CA** 签名的 **HTTPS** 证书

您可以在证书颁发机构签名并返回安全证书之后上传并安装它。您上传和安装的文件必须是签名版本的现有自签名证书。CA 签名证书有助于避免受到中间人攻击，且可提供比自签名证书更好的安全保护。

*什么 .开始之前

您必须已完成以下操作：

- 下载证书签名请求文件并由证书颁发机构签名
- 以 PEM 格式保存证书链
- 包括链中的所有证书，从 Unified Manager 服务器证书到根签名证书，包括存在的任何中间证书

您必须具有应用程序管理员角色。

如果为其创建 CSR 的证书的有效期超过 397 天，则 CA 将在签署并返回证书之前将其有效期缩短至 397 天

步骤

1. 在左侧导航窗格中，单击 常规 > **HTTPS** 证书。
2. 单击 安装 **HTTPS** 证书。
3. 在显示的对话框中，单击*选择文件……*以查找要上传的文件。
4. 选择文件，然后单击*安装*以安装文件。

   有关信息，请参见 "安装使用外部工具生成的 HTTPS 证书"。

示例证书链

以下示例显示了证书链文件的显示方式：

```
-----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-----
```

了解在 **Active IQ Unified Manager Unified Manager** 中使用外部工具生成的 **HTTPS** 证书

您可以安装自签名或 CA 签名的证书，这些证书是使用 OpenSSL、BoringSSL 、LetsEncrypt 等外部工具生成的。

您应该将私钥与证书链一起加载，因为这些证书是外部生成的公钥-私钥对。允许的密钥对算法是“RSA”和“EC”。

安装 **HTTPS** 证书 选项在常规部分下的 HTTPS 证书页面中提供。您上传的文件应采用以下输入格式。

1. Active IQ Unified Manager 主机所属服务器的私钥
2. 与私钥匹配的服务器证书
3. 反向直至根证书的 CA 证书，用于签署上述证书

使用 **EC** 密钥对加载证书的格式

允许的曲线为“prime256v1”和“secp384r1”。具有外部生成的 EC 对的证书示例：

```
 -----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-----
```

使用 **RSA** 密钥对加载证书的格式

属于主机证书的 RSA 密钥对的允许密钥大小为 2048、3072 和 4096。具有外部生成的 **RSA** 密钥对 的证书：

```
-----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-----
```

上传证书后，您应重新启动 Active IQ Unified Manager 实例以使更改生效。

上传外部生成的证书时的检查

系统在上传使用外部工具生成的证书时会执行检查。如果任何检查失败，则证书将被拒绝。此外，还包括对从产品内的 CSR 生成的证书以及使用外部工具生成的证书的验证。

- 输入中的私钥将根据输入中的主机证书进行验证。
- 根据主机的 FQDN 检查主机证书中的通用名称（CN）。
- 主机证书的公用名称（CN）不应为空或空白，也不应设置为 localhost。
- 有效期开始日期不应为将来日期，证书的有效期到期日期不应为过去日期。
- 如果存在中间 CA 或 CA，则证书的有效期开始日期不应在未来，有效期到期日期不应在过去。

输入中的私钥不应加密。如果存在任何已加密的私钥，则会被系统拒绝。

示例 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

示例 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

示例 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

如果证书安装失败，请参阅知识库 (KB) 文章：https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager 无法安装外部生成的证书"^]

证书管理的页面描述

了解 **Active IQ Unified Manager** 中的 **HTTPS** 证书页面

可使用 HTTPS 证书页面查看当前安全证书、下载证书签名请求、生成新的自签名 HTTPS 证书或安装新的 HTTPS 证书。

如果您尚未生成新的自签名 HTTPS 证书，则此页面上显示的证书就是在安装过程中生成的证书。

命令按钮

命令按钮可用于执行以下操作：

- 下载 **HTTPS** 证书签名请求

  下载当前安装的 HTTPS 证书的证书请求。您的浏览器会提示您保存 <hostname>.csr 文件，以便您可以将该文件提供给证书颁发机构进行签名。

- 安装 **HTTPS** 证书

  使您能够在证书颁发机构签名并返回后上传和安装安全证书。重新启动管理服务器后，新证书即生效。

- 重新生成 **HTTPS** 证书

  使您能够生成新的自签名 HTTPS 证书，以替换当前的安全证书。重新启动 Unified Manager 后，新证书即生效。

在 **Active IQ Unified Manager** 中重新生成 **HTTPS** 证书对话框

通过“重新生成 HTTPS 证书”对话框，您可以自定义安全信息，然后使用该信息生成新的 HTTPS 证书。

此页面上将显示当前证书信息。

“使用当前证书属性重新生成”和“更新当前证书属性”选项使您可以使用当前信息重新生成证书或使用新信息生成证书。

- 通用名称

  必需。要保护的完全限定域名 (FQDN)。

  在 Unified Manager 高可用性配置中，使用虚拟 IP 地址。

- 电子邮件

  可选。用于联系您组织的电子邮件地址；通常是证书管理员或 IT 部门的电子邮件地址。

- 公司

  可选。通常是公司的法定名称。

- 部门

  可选。公司部门名称。

- 城市

  可选。公司所在的城市位置。

- **State**

  可选。公司所在的州或省/自治区/直辖市位置（非缩写）。

- 国家/地区

  可选。公司所在的国家/地区位置。这通常是指国家/地区的两个字母的 ISO 代码。

- 备用名称

  必需。除了现有本地主机或其他网络地址以外，还可以使用其他非主域名来访问此服务器。每个替换名称均使用英文逗号进行分隔。

  如果要从证书的“备用名称”字段中删除本地标识信息，请选中 “Exclude local identifying information (e.g. localhost)” 复选框。选中此复选框时，仅在“备用名称”字段中使用您在该字段中输入的内容。留空时，生成的证书将完全没有“备用名称”字段。

- 密钥大小（密钥算法：**RSA**）

  密钥算法设置为 RSA。您可以选择一种密钥大小：2048、3072 或 4096 位。默认密钥大小设置为 2048 位。

- 有效期

  默认有效期为 397 天。如果您已从早期版本升级，您可能会看到以前的证书有效期保持不变。

有关详细信息，请参见"生成 HTTPS 证书"。

监控和管理存储

Active IQ Unified Manager 简介

了解Active IQ Unified Manager

Active IQ Unified Manager（以前称为 OnCommand Unified Manager）使您能够从单个界面监控和管理 ONTAP 存储系统的运行状况和性能。

Unified Manager 具有以下功能：

- 安装了 ONTAP 软件的系统的发现、监控和通知。
- 用于显示环境容量、安全性和性能运行状况的仪表板。
- 增强的警报、事件和阈值基础设施。
- 显示绘制工作负载活动随时间变化的详细图表；包括 IOPS（操作）、MBps（吞吐量）、延迟（响应时间）、利用率、性能容量和缓存比率。
- 识别过度使用集群组件的工作负载，以及性能受活动增加影响的工作负载。
- 提供可执行的建议纠正措施以解决某些突发事件和事件，并为某些事件提供“修复”按钮，以便您可以立即解决问题。
- 与 OnCommand Workflow Automation 集成以执行自动保护工作流程。
- 能够直接从 Unified Manager 创建新的工作负载（如 LUN 或文件共享），并分配性能服务级别，以定义使用该工作负载访问应用程序的用户的性能和存储目标。

了解 Active IQ Unified Manager 中的运行状况监控

Active IQ Unified Manager（以前称为 OnCommand Unified Manager）可帮助您通过集中式用户界面监控大量运行 ONTAP 软件的系统。Unified Manager 服务器基础架构提供可扩展性、可支持性以及增强的监控和通知功能。

Unified Manager 的主要功能包括监控、警报、管理集群的可用性和容量、管理保护功能以及将诊断数据捆绑并发送给技术支持。

您可以使用 Unified Manager 监控您的群集。当群集中出现问题时，Unified Manager 会通过事件通知您有关此类问题的详细信息。某些事件还为您提供了补救措施，您可以采取这些措施来纠正问题。您可以配置事件警报，以便在出现问题时通过电子邮件和 SNMP 陷阱通知您。

您可以使用 Unified Manager 将环境中的存储对象与标注关联起来以管理这些存储对象。您可以创建自定义标注，并通过规则将集群、存储虚拟机（SVM）和卷与标注动态关联起来。

您还可以使用容量和运行状况图表中提供的相应集群对象的信息来规划集群对象的存储要求。

物理和逻辑容量

Unified Manager 使用用于 ONTAP 存储对象的物理和逻辑空间的概念。

- 物理容量：物理空间是指卷中使用的物理存储块。由于存储效率功能（如重复数据删除和压缩）减少了数据，“物理已用容量”通常小于逻辑已用容量。
- 逻辑容量：逻辑空间是指卷中的可用空间（逻辑块）。逻辑空间是指如何使用理论空间，而不考虑重复数据删除或压缩的结果。“已用逻辑空间”是指已用物理空间加上已配置的存储效率功能（例如重复数据删除和压缩）所节省的空间。此测量值通常看起来大于已用物理容量，因为它未反映数据压缩和其他物理空间缩减。因此，总逻辑容量可能高于调配的空间。

容量测量单位

Unified Manager 基于 1024（2^{10}）字节的二进制单位计算存储容量。在 ONTAP 9.10.0 及更早版本中，这些单位显示为 KB、MB、GB、TB 和 PB。从 ONTAP 9.10.1 开始，它们在 Unified Manager 中显示为 KiB、MiB、GiB、TiB 和 PiB。

对于所有版本的 ONTAP，吞吐量使用的单位仍然是千字节/秒（Kbps）、兆字节/秒（Mbps）、千兆字节/秒（Gbps）或太字节/秒（Tbps）等等。

ONTAP 9.10.0 及更早版本的 **Unified Manager** 中显示的容量单位	**ONTAP 9.10.1** 的 **Unified Manager** 中显示的容量单位	计算方式	值（字节）
KB	KiB	1024	1024 字节
MB	MiB	1024 * 1024	1,048,576 字节
GB	GiB	1024 * 1024 * 1024	1,073,741,824 字节
TB	TiB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 字节

了解 **Active IQ Unified Manager** 中的性能监控

Active IQ Unified Manager（以前称为 OnCommand Unified Manager）为运行 NetApp ONTAP 软件的系统提供性能监控功能和事件根本原因分析。

Unified Manager 可帮助您识别过度使用集群组件并降低集群上其他工作负载性能的工作负载。通过定义性能阈值策略，您还可以为某些性能计数器指定最大值，以便在超出阈值时生成事件。Unified Manager 会提醒您这些性能事件，以便您可以采取纠正措施，并将性能恢复到正常运行水平。您可以在 Unified Manager UI 中查看和分析事件。

Unified Manager 可监控两种类型工作负载的性能：

- 用户定义的工作负载

  这些工作负载由您在集群中创建的 FlexVol 卷和 FlexGroup 卷组成。

- 系统定义的工作负载

  这些工作负载包括内部系统活动。

使用 **Active IQ Unified Manager REST API**

Active IQ Unified Manager 提供 REST API 来查看有关监控和管理存储环境的信息。API 还允许根据策略配置和管理存储对象。

您还可以使用 Unified Manager 支持的 API 网关在所有由 ONTAP 管理的集群上执行 ONTAP API。

有关 Unified Manager REST API 的信息，请参见 "Active IQ Unified Manager REST API 入门"。

Unified Manager 服务器的功能

了解 **Active IQ Unified Manager** 服务器

Unified Manager 服务器基础架构由数据收集单元、数据库和应用程序服务器组成。它提供基础架构服务，例如发现、监视、基于角色的访问控制（RBAC）、审核和记录。

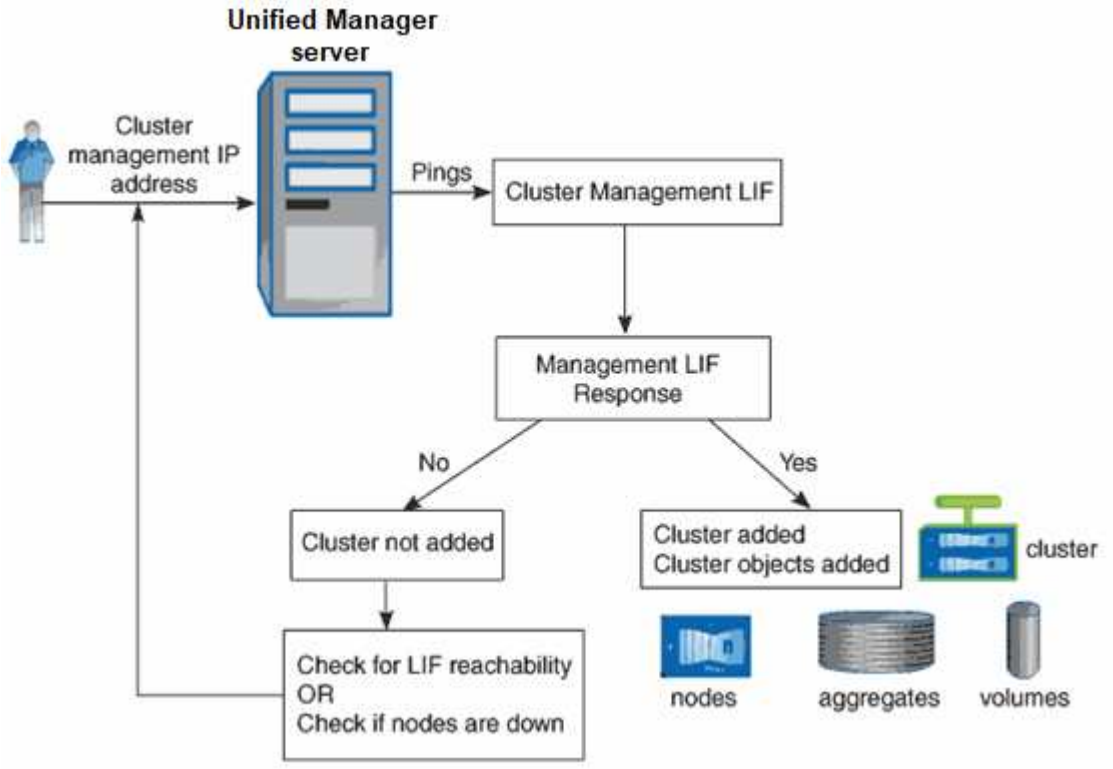
Unified Manager 收集群集信息，将数据存储在数据库中，并分析数据以查看是否存在任何群集问题。

了解 **Active IQ Unified Manager** 中的集群发现过程如何工作

将集群添加到 Unified Manager 后，服务器将发现集群对象并将其添加到其数据库中。了解发现过程的工作原理有助于您管理组织的集群及其对象。

默认监视间隔为 15 分钟：如果已将群集添加到 Unified Manager 服务器，则需要 15 分钟才能在 Unified Manager UI 中显示群集详细信息。

下图显示了 Active IQ Unified Manager 中的发现过程：



了解用户界面

了解 **Active IQ Unified Manager** 用户界面

Unified Manager 用户界面主要由一个仪表板组成，该仪表板提供被监控对象的概览视图。用户界面还提供查看所有集群对象的访问权限。

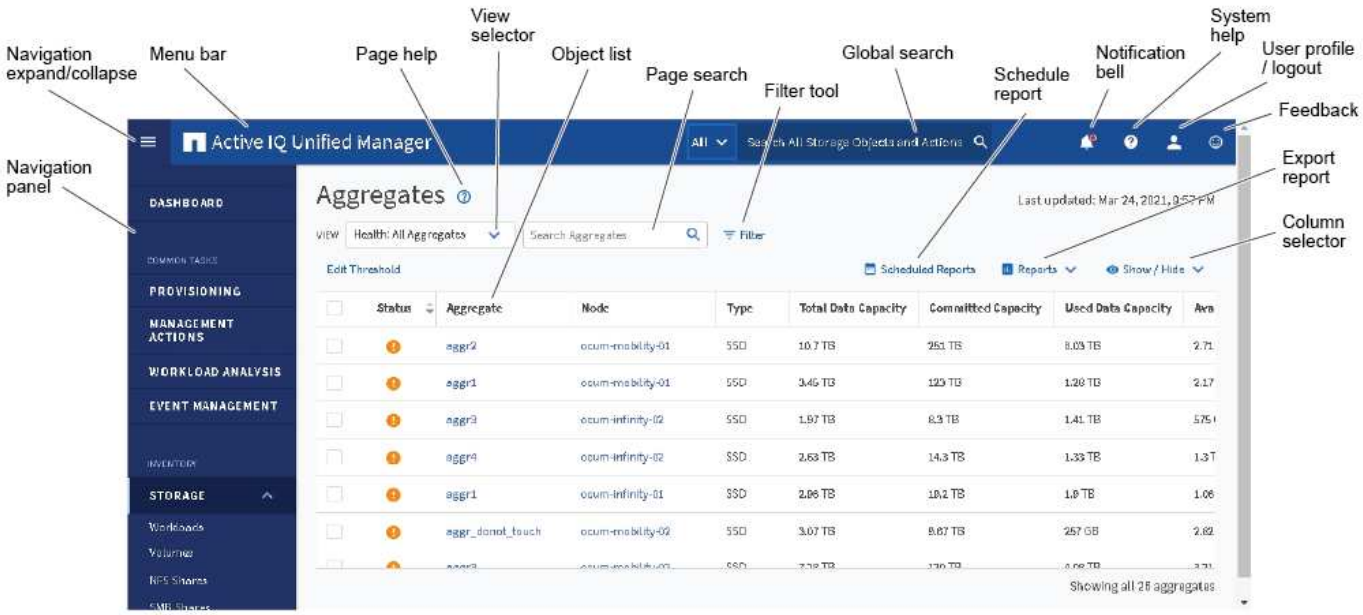
您可以选择首选视图，并根据需要使用操作按钮。您的屏幕配置将保存在工作区中，以便在启动 Unified Manager 时提供所需的所有功能。但是，当您从一个视图导航到另一个视图，然后返回时，视图可能不同。

Active IQ Unified Manager 中的典型窗口布局

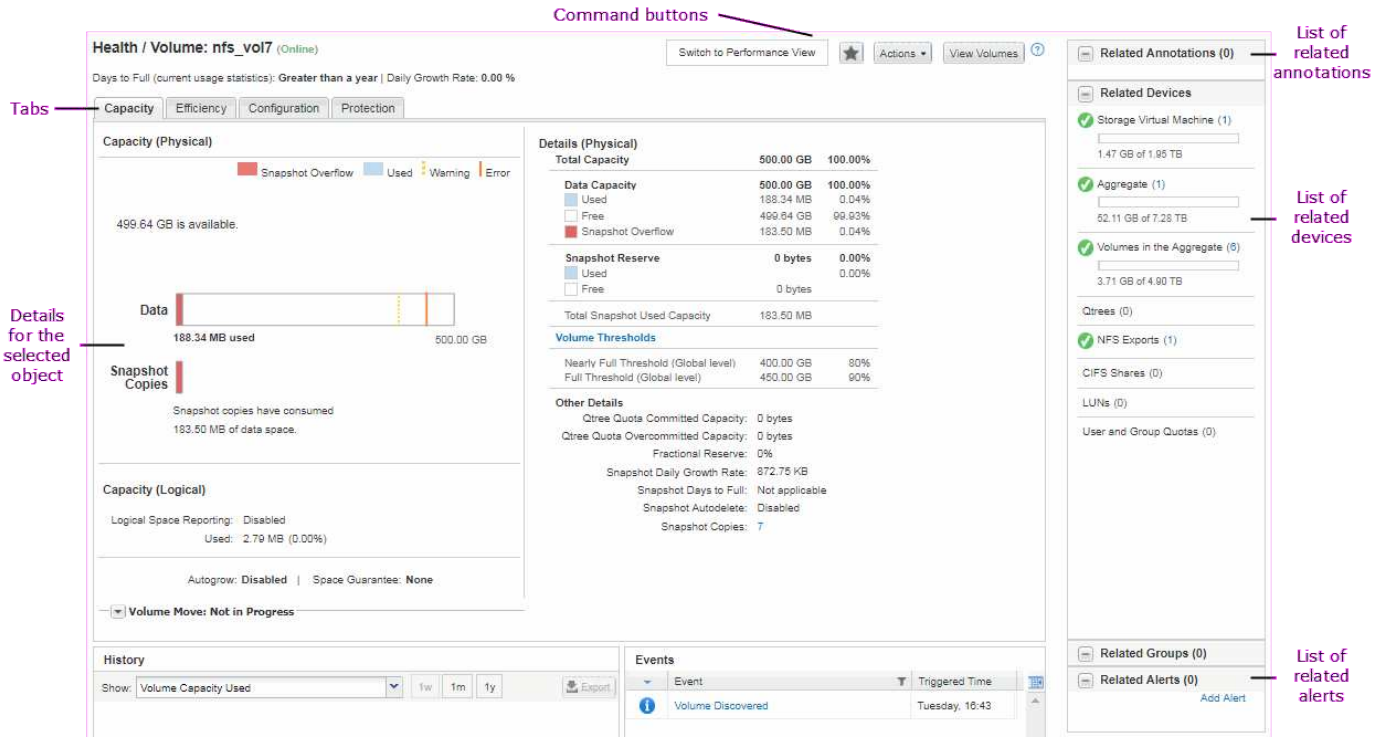
了解典型窗口布局有助于您有效地导航和使用 Active IQ Unified Manager。大多数 Unified Manager 窗口类似于两种常规布局之一：对象列表或详细信息。建议的显示设置至少为 1280 x 1024 像素。

并非每个窗口都包含以下图中的每个元素。

对象列表窗口布局



对象详细信息窗口布局



在 **Active IQ Unified Manager** 中自定义窗口布局

Active IQ Unified Manager 允许您自定义存储和网络对象页面上的信息布局。通过自定义窗口，您可以控制可查看的数据以及数据的显示方式。

- 排序

  您可以单击列标题来更改列条目的排序顺序。当您单击列标题时，该列将显示排序箭头（ 和 ）。

- 筛选

  您可以单击筛选器图标（ ）应用筛选器来自定义存储和网络对象页面上的信息显示，以便仅显示与所提供的条件匹配的条目。您可以在“筛选器”窗格中应用筛选器。

  通过“筛选器”窗格，您可以根据所选选项筛选大多数列。例如，在“运行状况：所有卷”视图中，您可以使用“筛选器”窗格，通过在“状态”下选择相应的筛选选项来显示所有离线卷。

  任何列表中与容量相关的列始终以适当的单位显示容量数据，并四舍五入到小数点后两位。这也适用于过滤容量列。例如，如果使用“运行状况：所有聚合”视图中“总数据容量”列中的筛选器来筛选大于 20.45 GB 的数据，则 20.454 GB 的实际容量将显示为 20.45 GB。同样，如果过滤的数据小于 20.45 GB，则 20.449 GB 的实际容量将显示为 20.45 GB。

  如果使用“运行状况：所有聚合”视图中“可用数据 %”列中的筛选器来筛选大于 20.45% 的数据，则 20.454% 的实际容量将显示为 20.45%。同样，如果筛选小于 20.45% 的数据，则 20.449% 的实际容量将显示为 20.45%。

- 隐藏或显示列

  您可以单击列显示图标（显示/隐藏）来选择要显示的列。选择合适的列后，您可以使用鼠标拖动它们来重新排序。

- 搜索

  您可以使用搜索框搜索某些对象属性，以帮助细化清单页面中的项目列表。例如，您可以输入 "cloud" 来细化卷清单页面中的卷列表，以查看其中包含单词 "cloud" 的所有卷。

- 导出数据

  您可以单击*报告*按钮（或*导出*按钮将数据导出为逗号分隔值 `(.csv)`文件、 `(.pdf)`文档或 Microsoft Excel `(.xlsx)`文件，并使用导出的数据构建报告。

使用 **Active IQ Unified Manager** 帮助

帮助包含有关 Active IQ Unified Manager 中包含的所有功能的信息。您可以使用目录、索引或搜索工具来查找有关功能及其使用方法的信息。

您可以从每个选项卡和 Unified Manager 用户界面的菜单栏获得帮助。

帮助中的搜索工具不适用于部分单词。

- 要了解特定字段或参数，请单击 。
- 要查看所有帮助内容，请在菜单栏中单击 > 帮助/文档。

  您可以通过展开导航窗格中目录的任何部分来查找更多详细信息。

- 要搜索帮助内容，请单击导航窗格中的*搜索*选项卡，键入要查找的单词或一系列单词，然后单击*开始！*
- 要打印“帮助”主题，请单击打印机图标。

在 **Active IQ Unified Manager** 中收藏您喜爱的帮助主题

在“帮助收藏夹”选项卡中，您可以将经常使用的帮助主题添加到书签中。帮助书签可快速访问您喜爱的主题。

步骤

1. 导航到要添加为收藏夹的“帮助”主题。
2. 单击*收藏夹*，然后单击*添加*。

在 **Active IQ Unified Manager** 中搜索存储对象

您可以使用菜单栏顶端的*搜索所有存储对象*字段快速访问特定对象。这种对所有对象进行全局搜索的方法使您能够按类型快速定位特定对象。搜索结果按存储对象类型排序，您可以使用下拉菜单按对象进一步筛选它们。

开始之前

- 必须具有以下角色之一才能执行此任务：操作员、应用程序管理员或存储管理员。
- 有效的搜索必须至少包含三个字符。

使用下拉菜单值“全部”时，全局搜索将显示在所有对象类别中找到的结果总数；每个对象类别最多可有 25 个搜

索结果。您可以从下拉菜单中选择特定对象类型，以优化特定对象类型内的搜索。在这种情况下，返回的列表不限于前 25 个对象。

可以搜索的对象类型包括：

- 集群
- 节点
- Storage VM
- 聚合
- 卷
- qtree
- SMB 共享
- NFS 共享
- 用户或组配额
- LUN 数
- NVMe 命名空间
- 启动程序组
- 启动程序
- 一致性组

输入工作负载名称将返回相应的卷或 LUN 类别下的工作负载列表。

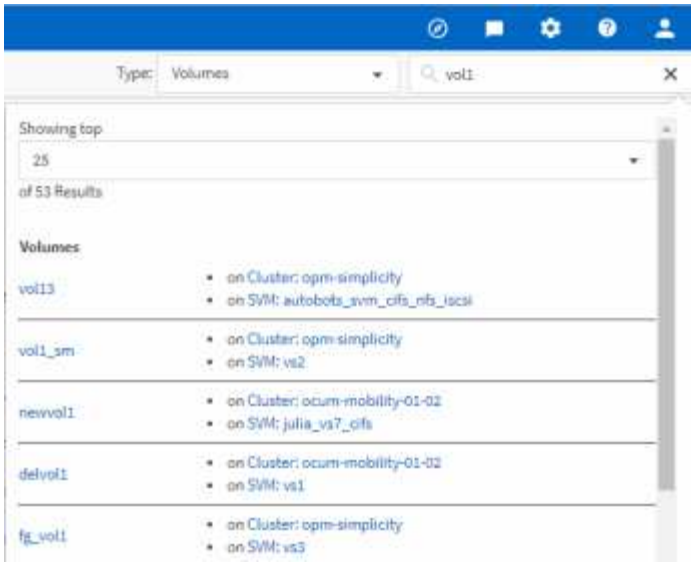
您可以单击搜索结果中的任何对象以导航到该对象的“运行状况”详细信息页面。如果没有对象的直接运行状况页面，则会显示父对象的运行状况页面。例如，在搜索特定 LUN 时，将显示 LUN 所在的 SVM 详细信息页面。

端口和 LIF 在全局搜索栏中不可搜索。

步骤

1. 从菜单中选择对象类型，以仅针对单一对象类型细化搜索结果。
2. 在 **Search all Storage Objects** 字段中输入对象名称的至少三个字符。

   在此示例中，下拉框选择了 Volumes 对象类型。在 搜索所有存储对象 字段中键入 "vol1" 将显示名称包含这些字符的所有卷的列表。



将存储数据导出为 **Active IQ Unified Manager** 中的报告

您可以以各种输出格式导出存储数据，然后使用导出的数据生成报告。例如，如果有 10 个关键事件尚未解决，则可以从事件管理清单页面导出数据以创建报告，然后将报告发送给可以解决问题的管理员。

您可以从 存储 和 网络 清单页面将数据导出为 `.csv`文件、 `.xlsx`文件或 `.pdf`文档，并使用导出的数据生成报告。产品中还有其他位置只能生成 `.csv`或 `.pdf`文件。

步骤

1. 请执行以下操作之一：

如果要导出……	操作
存储对象清单详细信息	从左侧导航菜单中单击 存储 或 网络，然后选择一个存储对象。选择系统提供的视图之一，或您已创建的任何自定义视图。
QoS 策略组详细信息	点击左侧导航菜单中的 存储 > **QoS** 策略组。
存储容量和保护历史记录详细信息	单击*存储* > 聚合*或*存储 > 卷，然后选择单个聚合或卷。
事件详情	从左侧导航菜单中单击*事件管理*。
存储对象前 10 名性能详细信息	单击 存储 > 集群 > 性能：所有集群，然后选择一个集群并选择 表现最佳者 选项卡。然后选择一个存储对象和性能计数器。

2. 单击*报告*按钮（或某些 UI 页面中的*导出*按钮）。
3. 单击 下载 **CSV**、下载 **PDF** 或 下载 **Excel** 确认导出请求。

   从“最高性能对象”选项卡中，您可以选择下载正在查看的单个集群或数据中心中所有集群的统计信息报告。

   此文件已下载。

4. 在相应的应用程序中打开文件。

相关信息

"运行状况/集群清单页面"

"计划报告"

在 **Active IQ Unified Manager** 中筛选清单页面内容

您可以在 Unified Manager 中筛选清单页面数据，以根据特定条件快速查找数据。您可以使用筛选功能来缩小 Unified Manager 页面的内容范围，以仅显示您感兴趣的结果。这提供了一种非常有效的方法，仅显示您感兴趣的数据。

使用 过滤 根据您的偏好自定义网格视图。可用的过滤器选项基于在网格中查看的对象类型。如果当前已应用过滤器，则已应用过滤器的数量将显示在“过滤器”按钮的右侧。

支持三种类型的过滤器参数。

参数	验证
字符串（文本）	运算符是*包含*、以……开头、以……结尾*和*不包含。
数字	运算符包括*大于*、小于、在最后*和*之间。
枚举（文本）	运算符是 **is** 和 **is not**。

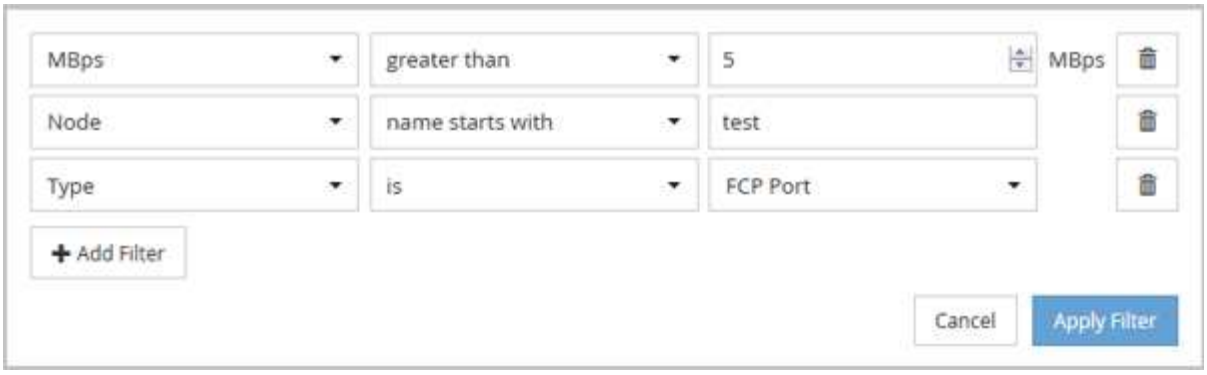
每个筛选器都需要 Column（列）、Operator（运算符）和 Value（值）字段；可用的筛选器反映当前页面上的可筛选列。您最多可以应用四个筛选器。筛选结果基于组合的筛选器参数。筛选结果适用于筛选搜索中的所有页面，而不仅仅是当前显示的页面。

您可以使用“过滤”面板添加过滤器。

1. 在页面顶部，单击*筛选*按钮。此时将显示筛选面板。
2. 单击左侧下拉列表并选择一个对象；例如，*Cluster* 或性能计数器。
3. 单击中部下拉列表，然后选择要使用的运算符。
4. 在最后一个列表中，选择或输入一个值以完成此对象的筛选器。
5. 要添加其他过滤器，请单击 **+**添加过滤器。此时将显示一个额外的过滤器字段。使用前述步骤中描述的过程完成此过滤器。请注意，添加第四个过滤器后，**+**添加过滤器 按钮不再显示。
6. 单击*应用过滤器*。过滤器选项将应用于网格，过滤器的数量将显示在“过滤器”按钮的右侧。
7. 使用“筛选”面板，通过单击要删除的筛选器右侧的垃圾箱图标来删除单个筛选器。
8. 要删除所有过滤器，请点击过滤面板底部的*重置*。

筛选示例

该图显示了带有三个筛选条件的“筛选”面板。当您的筛选条件少于最多四个时，会显示 **+**添加筛选条件 按钮。



单击 应用过滤器 后，过滤面板将关闭，应用您的过滤器，并显示已应用的过滤器数量（ 3 ）。

通过 **Active IQ Unified Manager** 中的通知铃查看活动事件

菜单栏中的通知铃（）提供了一种快速查看 Unified Manager 正在跟踪的最重要活动事件的方法。

活动事件列表提供了一种查看所有集群上的关键事件、错误事件、警告事件和升级事件总数的方法。此列表包括过去 7 天的事件，不包括信息事件。您可以单击链接以显示您最感兴趣的事件列表。

请注意，当无法访问集群时，Unified Manager 会在此页面中显示此信息。您可以通过单击 详细信息 按钮查看有关无法访问的集群的详细信息。此操作将打开事件详细信息页面。此页面上还会显示规模监控问题，例如管理站上的空间或 RAM 不足。

步骤

1. 从菜单栏中，单击 。
2. 要查看任何活动事件的详细信息，请单击事件文本链接，例如“2 个容量”或“4 个性能”。

从仪表板监控和管理集群

通过 **Active IQ Unified Manager** 中的信息板监控和管理集群

仪表板提供有关受监控 ONTAP 系统当前运行状况的累积概览信息。仪表板提供“`panels`”，使您能够评估正在监控的集群的整体容量、性能和安全运行状况。

此外，您可以直接从 Unified Manager 用户界面修复某些 ONTAP 问题，而不必使用 ONTAP System Manager 或 ONTAP CLI。

可从信息板顶部选择让这些面板显示所有受监控集群的信息，还是仅显示单个集群的信息。您可以先查看所有集群的状态，然后深入查看各个集群以查看相关详细信息。

根据您的配置，下列部分面板可能不会显示在此页面上。

面板	问题描述
管理操作	当 Unified Manager 可以诊断并确定问题的单一解决方案时，这些解决方案将通过 修复 按钮显示在此面板中。
容量	显示本地层和云层的总容量和已用容量，以及本地容量达到上限之前的天数。
性能容量	显示每个集群的性能容量值，以及性能容量达到上限之前的天数。
工作负载 IOPS	显示当前在特定 IOPS 范围内运行的工作负载总数。
工作负载性能	显示分配给每个已定义性能服务级别的符合和不符合工作负载的总数。
安全性	显示符合或不符合的群集数量、符合或不符合的 SVM 数量以及已加密或未加密的卷数量。
数据保护	显示受 SVM-DR 关系保护的 Storage VM 数量、受 SnapMirror 关系保护的卷、受 Snapshot 保护的卷以及受 MetroCluster 保护的集群。
使用情况概述	显示按最高 IOPS、最高吞吐量 (MBps) 或最高已用物理容量排序的集群。

了解 **Active IQ Unified Manager** 仪表板页面

仪表板页面有“面板”，显示您正在监控的集群的高级容量、性能和安全运行状况。此页面还提供了一个管理操作面板，其中列出了 Unified Manager 可以为解决某些事件而进行的修复。

大多数面板还显示该类别中的活动事件数，以及过去 24 小时内添加的新事件数。此信息可帮助您确定可能需要进一步分析以解决事件的集群。单击事件会显示热门事件，并提供指向事件管理清单页面的链接，该页面已过滤以显示该类别中的活动事件。

在仪表板的顶部，您可以选择面板是否显示所有受监控集群（“所有集群”）或单个集群的信息。您可以先查看所有集群的状态，然后在需要查看详细信息时深入查看单个集群。

下面列出的一些面板根据您的配置显示在控制面板上。

管理操作面板

Unified Manager 可以彻底诊断某些问题并提供单一解决方案。如果可用，这些解决方案将通过 **Fix It** 或 **Fix All** 按钮显示在此面板中。您可以立即从 Unified Manager 修复这些问题，而不必使用 ONTAP System Manager 或 ONTAP CLI。要查看所有问题，请单击“请参见” "直接从 Unified Manager 修复 ONTAP 问题" 以了解更多信息。

容量面板

查看所有集群时，此面板显示每个集群的物理已用容量（应用存储效率节约后）和物理可用容量（不包括潜在的存储效率节约）、预计磁盘已满的天数以及基于配置的 ONTAP 存储效率设置的数据缩减率（不包括 Snapshot 副本）。它还列出了任何已配置云层的已用容量。单击条形图将转到该集群的聚合清单页面。单击“Days To Full”文本将显示一条消息，标识剩余容量天数最少的聚合；单击聚合名称可查看更多详细信息。

查看单个集群时，此面板显示按本地层上的每个单独磁盘类型排序的数据聚合以及云层的物理已用容量和物理可用容量。单击磁盘类型的条形图将转到使用该磁盘类型的卷的卷清单页面。

性能容量面板

查看所有集群时，此面板显示每个集群的性能容量值（过去 1 小时的平均值）以及性能容量达到上限（基于每日增长率）的天数。单击条形图将转到该集群的节点清单页面。请注意，节点清单页面显示过去 72 小时的平均性能容量。单击“Days To Full”文本将显示一条消息，标识剩余性能容量天数最少的节点；单击节点名称可查看更多详细信息。

查看单个集群时，此面板会显示集群性能容量使用百分比、总 IOPS 和总吞吐量 (MB/s) 值，以及这三个指标预计将达到上限的天数。

Workload IOPS 面板

查看单个集群时，此面板显示当前在特定 IOPS 范围内运行的工作负载总数，并在将光标悬停在图表上时显示每种磁盘类型的数量。

工作负载性能面板

此面板显示分配给每个性能服务级别（PSL）策略的符合和不符合的工作负载的总数。它还显示未分配 PSL 的工作负载数量。单击条形图将转到“工作负载”页面中分配给该策略的符合的工作负载。单击条形图后面的数字将转到分配给该策略的符合和不符合的工作负载。

安全面板

安全面板显示所有群集或单个群集的高级安全状态，具体取决于您当前的视图。此面板显示：

- 过去 24 小时内收到的安全事件列表。单击某个事件可在“事件详细信息”页面上查看详细信息
- 集群安全状态（合规和不合规集群的计数）
- storage VM 安全状态（合规和不合规的 storage VM 计数）
- 卷加密状态（已加密或未加密的卷的计数）
- 卷反勒索软件状态（启用或禁用反勒索软件的卷数）

您可以单击合规和不合规集群、存储 VM、加密和未加密卷以及卷防勒索软件状态的条形图，转到相应页面并查看已过滤集群、存储 VM 和卷的安全详细信息。

合规性基于 "适用于 ONTAP 9 的 NetApp 安全强化指南"。单击面板顶部的右箭头可查看安全页面上所有集群的安全详细信息。有关信息，请参见"查看集群和 Storage VM 的详细安全状态"。

数据保护面板

此面板显示数据中心中单个或所有集群的数据保护摘要。它显示过去24小时内在 ONTAP 中引发的数据保护事件、MetroCluster 事件以及活动事件的总数。单击每个事件的链接将转到“事件详细信息”页面。您可以单击 查看全部 链接，在事件管理清单页面中查看所有活动保护事件。该面板显示：

- 受 Snapshot 副本保护的集群或数据中心内所有集群中的卷数。
- 受 SnapMirror 关系保护的集群或数据中心内所有集群中的卷数。对于 SnapMirror 关系，将考虑源集群上的卷数。

- 通过 IP 或 FC MetroCluster 配置保护的数据中心中的集群或所有集群的数量。
- 基于延迟状态的具有 SnapMirror 恢复点目标（RPO）延迟的卷关系数量。

您可以悬停鼠标以查看相应的计数和图例。您可以单击面板顶部的右箭头，查看数据保护页面上单个或所有集群的详细信息。此外，您还可以单击：

- 未受保护卷和受 Snapshot 副本保护的卷的条形图，转到“卷”页面并查看详细信息。
- 受 MetroCluster 配置保护或不受保护的集群的条形图，转到“集群”页面并查看详细信息。
- 所有关系的条形图可转到“关系”页面，其中的详细信息将根据源集群进行筛选。

有关详细信息，请参见"查看卷保护状态"。

使用概述面板

在查看所有集群时，您可以选择按最高 IOPS、最高吞吐量（MB/秒）或最高已用物理容量对集群进行排序。

在查看单个集群时，您可以选择按最高 IOPS、最高吞吐量（MB/s）或最高已用逻辑容量对工作负载进行排序。

相关信息

"使用 Unified Manager 自动修复功能解决问题"

"显示性能事件的相关信息"

"使用性能容量和可用 IOPS 信息管理性能"

"卷 / 运行状况详细信息页面"

"性能事件分析和通知"

"事件严重性类型的说明"

"性能事件源"

"管理集群安全目标"

"从性能集群登录页面监控集群性能"

"使用性能清单页面监控性能"

直接从 **Unified Manager** 修复或管理 **ONTAP** 问题

直接从 **Active IQ Unified Manager** 管理 **ONTAP** 问题或功能

您可以直接从 Unified Manager 用户界面修复某些 ONTAP 问题或管理某些 ONTAP 功能，而不必使用 ONTAP System Manager 或 ONTAP CLI。“管理操作”选项可修复触发 Unified Manager 事件的许多 ONTAP 问题。

您可以通过选择左侧导航窗格中的*管理操作*选项，直接从管理操作页面解决问题。管理操作也可以从仪表板上的管理操作面板、事件详细信息页面和左侧导航菜单上的工作负载分析选择中获得。

Unified Manager 可以彻底诊断某些问题并提供单一解决方案。对于某些 ONTAP 功能，例如反勒索软件监控，Unified Manager 会执行内部检查并建议具体操作。如果可用，这些解决方案将通过*修复*按钮显示在管理操作中。单击*修复*按钮以解决此问题。您必须具有应用程序管理员或存储管理员角色。

Unified Manager 将 ONTAP 命令发送到集群以进行请求的修复。修复完成后，事件将被废弃。

某些管理操作使您能够使用 全部修复 按钮修复多个存储对象上的相同问题。例如，可能有 5 个卷具有“卷空间已满”事件，可以通过单击“启用卷自动增长”的 全部修复 管理操作来解决。只需单击一下，即可在 5 个卷上修复此问题。

有关可通过使用自动修正进行管理的 ONTAP 问题和功能的信息，请参见 "Unified Manager 可以解决哪些问题"。

了解 **Active IQ Unified Manager** 中的**"Fix It"**和**"Fix All"**按钮选项

管理操作页面为您提供*修复它*或*全部修复*按钮，以修复通过事件通知 Unified Manager 的问题。

我们建议您根据需要单击按钮以解决问题。但是，如果您不确定是否要按照 Unified Manager 的建议解决此问题，则可以执行以下操作：

您希望做什么？	操作
让 Unified Manager 解决所有已识别对象上的问题。	单击 全部修复 按钮。
此时请勿修复任何已识别对象的问题，并在再次引发事件之前隐藏此管理操作。	单击向下箭头并单击*全部关闭*。
仅修复部分已识别对象上的问题。	单击管理操作的名称以展开列表并显示所有单个 **Fix It** 操作。然后按照步骤修复或取消单个管理操作。

您希望做什么？	操作
让 Unified Manager 解决此问题。	单击 **Fix It** 按钮。
目前不要修复此问题，并在再次引发事件之前隐藏此管理操作。	单击向下箭头并单击 **Dismiss**。
显示此事件的详细信息以更好地了解此问题。	• 单击 **Fix It** 按钮，并在生成的对话框中查看将要应用的修复。 • 单击向下箭头，然后单击*查看事件详细信息*以显示事件详细信息页面。 然后，如果您想解决此问题，请在任意一个结果页面中单击 修复它。
显示此存储对象的详细信息以更好地了解此问题。	单击存储对象的名称可在“性能资源管理器”或“运行状况详细信息”页面中显示详细信息。

在某些情况下，修复会反映在接下来的 15 分钟配置轮询中。在其他情况下，可能需要长达数小时才能验证配置更改并使事件过时。

要查看已完成或正在进行的管理操作列表，请单击过滤器图标并选择*已完成*或*正在进行*。

修复所有操作以串行方式运行，因此当您查看 进行中 面板时，某些对象的状态将为 进行中，而其他对象的状态将为 计划；这意味着它们仍在等待实施。

查看要在 **Active IQ Unified Manager** 中修复的管理操作状态

您可以在“管理操作”页面中查看您选择修复的所有管理操作的状态。在 Unified Manager 向集群发送 ONTAP 命令后，大多数操作都会很快显示为*已完成*。但是，某些操作（例如移动卷）可能需要更长时间。

“管理操作”页面上有三个可用的筛选器：

- *已完成*显示成功完成的管理操作和失败的管理操作。*失败*的操作提供了失败的原因，以便您可以手动解决问题。
- *进行中*既显示正在实施的管理行动，也显示计划实施的管理行动。
- *推荐*显示当前对所有受监控集群处于活动状态的所有管理操作。

步骤

1. 单击左侧导航窗格中的*管理操作*。或者，单击*仪表板*上*管理操作*面板顶部的 ，然后选择要查看的视图。

   此时将显示管理操作页面。

2. 您可以单击*描述*字段中管理操作旁边的插入符号图标，查看有关问题的详细信息以及用于解决问题的命令。
3. 要查看任何*失败*的操作，请对*已完成*视图中的*状态*列进行排序。您可以使用*筛选器*工具来实现相同目的。
4. 如果要查看有关失败的管理操作的更多信息，或者如果决定要修复建议的管理操作，则可以在单击管理操作旁边的插入符号图标后，单击展开区域中的*查看事件详细信息*。该页面上提供了一个*修复它*按钮。

了解 **Active IQ Unified Manager** 可以解决的 **ONTAP** 问题

通过使用 Active IQ Unified Manager 的自动修复功能，您可以选择通过 Unified Manager 有效解决某些 ONTAP 问题或管理某些 ONTAP 功能，例如反勒索软件监控。

此表介绍了这些 ONTAP 问题或功能，您可以直接通过 Unified Manager Web UI 上的 **Fix It** 或 **Fix All** 按钮进行管理。

事件名称和描述	管理操作	“修复”操作
卷空间全满 卷空间即将用尽，并且已超出容量全满阈值。此阈值默认设置为卷大小的 90%。	启用卷自动增长	Unified Manager 确定此卷未配置卷自动增长功能，因此启用此功能，以便卷在需要时能够扩展容量。
索引节点全满 此卷已用完 inode，无法接受任何新文件。	增加卷上的 inode 数量	将卷上的 inode 数量增加 2%。

事件名称和描述	管理操作	“修复”操作
检测到存储层策略不匹配 卷中有大量非活动数据，当前分层策略设置为“仅快照”或“无”。	启用自动云分层	由于卷已驻留在 FabricPool 上，因此它将分层策略更改为“auto”，以便将非活动数据移动到成本较低的云层。
检测到存储层不匹配 该卷有大量非活动数据，但它不驻留在启用云的存储层（FabricPool）上。	更改卷的存储层	将卷移动到启用了云的存储层，并将分层策略设置为“auto”，以将非活动数据移动到云层。
已禁用审核日志 存储 VM 未启用审核日志	为 Storage VM 启用审核日志记录	在 Storage VM 上启用审核日志记录。 请注意，存储虚拟机必须已配置本地或远程审核日志位置。
已禁用登录横幅 应启用集群的登录横幅，通过明确说明访问限制来提高安全性。	为集群设置登录横幅	将集群登录横幅设置为“`Access restricted to authorized users`”。
已禁用登录横幅 应启用 storage VM 的登录横幅，以通过明确说明访问限制来提高安全性。	为存储虚拟机设置登录横幅	将 storage VM 登录横幅设置为“仅限授权用户访问”。
SSH 正在使用不安全密码 后缀为“-cbc”的密码被认为是不安全的。	从集群中删除不安全的密码	从集群中删除不安全的密码（如 aes192-cbc 和 aes128-cbc）。
SSH 正在使用不安全密码 后缀为“-cbc”的密码被认为是不安全的。	从存储虚拟机中删除不安全的密码	从存储 VM 中删除不安全的密码套件——例如 aes192-cbc 和 aes128-cbc。
已禁用 AutoSupport HTTPS 传输 用于向技术支持发送 AutoSupport 消息的传输协议应加密。	将 HTTPS 设置为 AutoSupport 消息的传输协议	将 HTTPS 设置为集群上 AutoSupport 消息的传输协议。
已超过集群负载不平衡阈值 表示集群中各节点之间的负载不均衡。当节点之间已用性能容量的差异超过 30% 时，将生成此事件。	平衡集群工作负载	Unified Manager 确定从一个节点移动到另一个节点的最佳卷以缓解不平衡状况，然后移动该卷。
已超过集群容量不平衡阈值 指示此集群中的聚合之间的容量不平衡。此事件在聚合之间的已用容量差异超过 70% 时生成。	平衡集群容量	Unified Manager 确定从一个聚合移动到另一个聚合的最佳卷，以缓解不平衡状况，然后移动卷。

事件名称和描述	管理操作	“修复”操作
已违反性能已用容量阈值 表示如果不降低一个或多个高活动工作负载的利用率，节点上的负载可能会被过度利用。当节点性能容量已用值超过 100% 且持续超过 12 小时时，将生成此事件。	限制节点上的高负载	Unified Manager 识别具有最高 IOPS 的卷，并使用历史预期和峰值 IOPS 级别应用 QoS 策略，以减少节点上的负载。
已违反动态事件警告阈值 表示由于某些工作负载的负载异常高，节点已处于过载状态。	减少节点中的过载	Unified Manager 识别具有最高 IOPS 的卷，并使用历史预期和峰值 IOPS 级别应用 QoS 策略，以减少节点上的负载。
无法接管 当前已禁用故障转移，因此在发生中断或重新启动期间可能无法访问节点的资源，直到节点恢复可用为止。	启用节点故障转移	Unified Manager 发送适当的命令以在集群中的所有节点上启用故障转移。
选项 Cf.takeover.on_panic 已配置为关闭 nodeshell 选项 "cf.takeover.on_panic" 设置为 **off**，这可能会导致 HA 配置的系统出现问题。	在系统崩溃时启用接管	Unified Manager 向集群发送相应的命令，以将此设置更改为 **on**。
禁用 nodeshell 选项 snapmirror.enable 旧的 nodeshell 选项“snapmirror.enable”设置为 **on**，这可能会在升级到 ONTAP 9.3 或更高版本后导致启动过程中出现问题。	将 snapmirror.enable 选项设置为 off	Unified Manager 向集群发送相应的命令，以将此设置更改为*关闭*。
已启用 Telnet 表示可能存在安全问题，因为 Telnet 不安全并以未加密的方式传递数据。	禁用 Telnet	Unified Manager 向集群发送相应的命令以禁用 Telnet。
配置 storage VM 反勒索软件学习 定期检查具有反勒索软件监控许可证的集群。验证存储虚拟机是否仅支持此类集群中的 NFS 或 SMB 卷。	将 Storage VM 置于反勒索软件监控 `learning`模式	Unified Manager 通过集群管理控制台将存储虚拟机的反勒索软件监控设置为 `learning`状态。在存储虚拟机上创建的所有新卷上的反勒索软件监控将自动移至学习模式。通过此功能，ONTAP 可以了解卷上的活动模式，并检测由于潜在的恶意攻击而导致的异常。

事件名称和描述	管理操作	“修复”操作
配置卷反勒索软件学习 定期检查具有反勒索软件监控许可证的集群。验证卷在此类集群中是否仅支持 NFS 或 SMB 服务。	将卷设置为反勒索软件监控 `learning`模式	Unified Manager 通过集群管理控制台将这些卷的反勒索软件监控设置为 `learning`状态。通过此功能，ONTAP 可以了解卷上的活动模式，并检测由于潜在恶意攻击而导致的异常。
启用卷反勒索软件 定期检查具有反勒索软件监控许可证的群集。检测卷是否处于反勒索软件监控的 `learning`模式超过 45 天，并确定将其置于活动模式的可能性。	将卷设置为反勒索软件监控 `active`模式	Unified Manager 通过集群管理控制台将卷上的反勒索软件监控设置为 `active`。通过此功能，ONTAP 可以了解卷上的活动模式，检测由于潜在恶意攻击而导致的异常，并为数据保护操作创建警报。
禁用卷反勒索软件 定期检查具有反勒索软件监控许可证的集群。在对卷进行主动反勒索软件监控期间检测重复通知（例如，在 30 天内返回有关潜在勒索软件攻击的多个警告）。	禁用卷上的反勒索软件监控	Unified Manager 通过集群管理控制台禁用对卷的反勒索软件监控。

使用 **Active IQ Unified Manager** 中的脚本覆盖管理操作

您可以创建自定义脚本并将其关联到警报，以针对特定事件采取特定操作，而不是在“管理操作”页面或 Unified Manager 仪表板上选择可用于它们的默认管理操作。

如果要对事件类型采取特定操作，并选择不将其作为 Unified Manager 提供的管理操作功能的一部分进行修复，则可以为特定操作配置自定义脚本。然后，您可以将脚本与该事件类型的警报相关联，并单独处理此类事件。在此情况下，不会在“管理操作”页面或 Unified Manager 仪表板上为该特定事件类型生成管理操作。

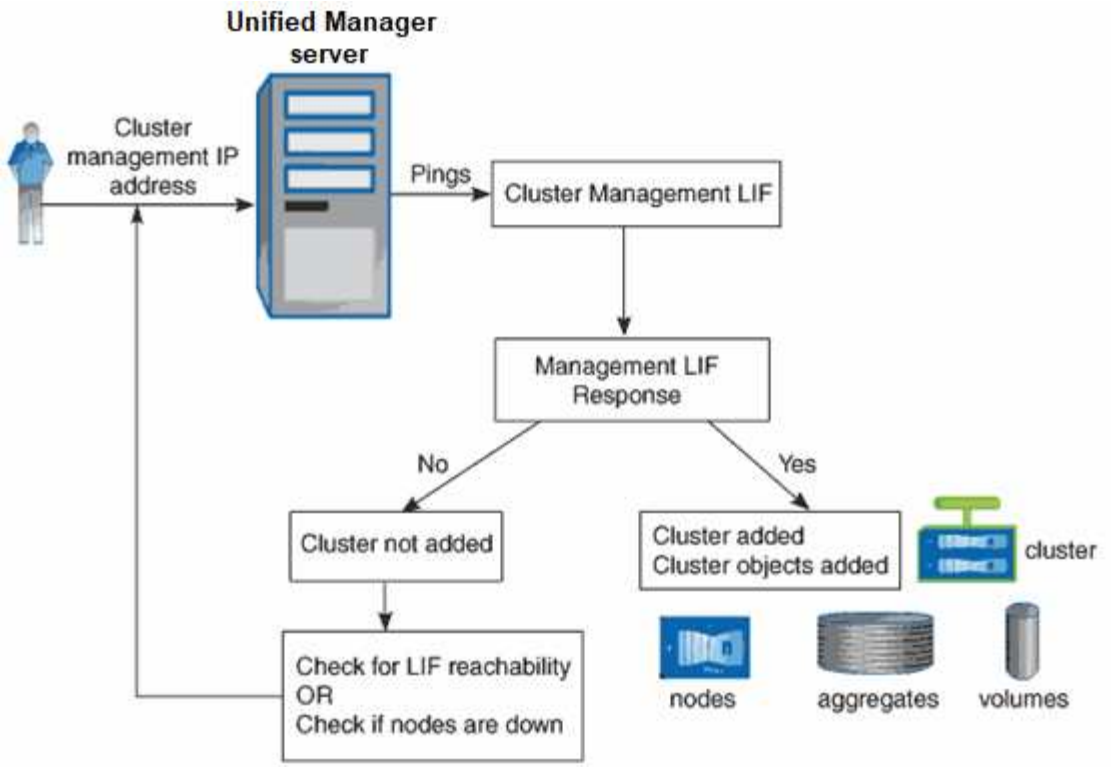
管理集群

了解 **Active IQ Unified Manager** 中的集群发现过程如何工作

将集群添加到 Unified Manager 后，服务器将发现集群对象并将其添加到其数据库中。了解发现过程的工作原理有助于管理组织的集群及其对象。

收集集群配置信息的监控间隔为 15 分钟。例如，添加集群后，需要 15 分钟才能在 Unified Manager UI 中显示集群对象。对集群进行更改时，此时间范围同样适用。例如，如果向集群中的 SVM 添加两个新卷，则在下一个轮询间隔（可能长达 15 分钟）之后，您会在 UI 中看到这些新对象。

下图显示了发现过程：



发现新集群的所有对象后，Unified Manager 将开始收集前 15 天的历史性能数据。这些统计数据通过数据连续性收集功能进行收集。此功能可在集群添加后立即为您提供超过两周的集群性能信息。数据连续性收集周期完成后，将默认每五分钟收集一次实时集群性能数据。

由于收集 15 天的性能数据会占用大量 CPU 资源，因此建议您错开添加新集群的时间，以便不会在过多的集群上同时运行数据连续性收集轮询。

查看 **Active IQ Unified Manager** 监控的集群列表

您可以使用“集群设置”页面查看集群清单。您可以查看有关集群的详细信息，例如其名称或 IP 地址以及通信状态。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 集群设置。

   将显示由 Unified Manager 管理的存储环境中的所有集群。集群列表按收集状态严重级别列排序。您可以单击列标题，按不同列对集群进行排序。

向 **Active IQ Unified Manager** 添加集群

您可以将集群添加到 Active IQ Unified Manager 以便可以监视该集群。这包括能够获取集群信息，例如集群的运行状况、容量、性能和配置，以便您可以查找并解决可能发生的任何问题。

开始之前

- 您必须具有应用程序管理员角色或存储管理员角色。
- 您必须具有下列信息：
  - Unified Manager 支持本地 ONTAP 集群、ONTAP Select、Cloud Volumes ONTAP。
  - 您必须知道集群的主机名或集群管理 IP 地址（IPv4 或 IPv6）。

    如果使用主机名，它必须解析为集群管理 LIF 的集群管理 IP 地址。如果使用节点管理 LIF，则操作会失败。
  - 您必须知道访问集群的用户名和密码。

    此帐户必须具有 *admin* 角色，应用程序访问权限设置为 *ontapi*、*amqp*、*console* 和 *http*。
  - 您必须知道使用 HTTPS 协议连接到集群所要使用的端口号（通常为端口 443）。
  - 此集群必须运行 ONTAP 9.9 或更高版本的软件。
  - 必须在 Unified Manager 服务器上有足够的空间。如果已占用超过 90% 的空间，则无法向服务器添加集群。
  - 您拥有所需的证书：

    SSL (HTTPS) 证书：此证书由 Unified Manager 拥有。全新安装 Unified Manager 时，会生成默认的自签名 SSL (HTTPS) 证书。NetApp 建议将其升级为 CA 签名证书，以获得更好的安全性。如果服务器证书过期，您应重新生成该证书并重新启动 Unified Manager，以便服务采用新证书。有关重新生成 SSL 证书的详细信息，请参见 "生成 HTTPS 安全证书"。

    EMS 证书：此证书归 Unified Manager 所有。它在对从 ONTAP 接收的 EMS 通知进行身份验证时使用。

    双向 **TLS** 通信证书：在 Unified Manager 和 ONTAP 之间的双向 TLS 通信期间使用。系统会根据 ONTAP 版本为集群启用基于证书的身份验证。如果集群运行的 ONTAP 版本低于 9.5，则不会启用基于证书的身份验证。

    如果您要更新早期版本的 Unified Manager，则不会为集群自动启用基于证书的身份验证。但是，您可以通过修改并保存集群详细信息来启用它。如果证书过期，您应重新生成证书以整合新证书。有关查看和重新生成证书的详细信息，请参见"编辑集群"。

    - 您可以从 Web UI 添加集群，并自动启用基于证书的身份验证。
    - 您可以通过 Unified Manager CLI 添加集群，默认情况下不会启用基于证书的身份验证。如果使用 Unified Manager CLI 添加集群，则需要使用 Unified Manager UI 编辑集群。您可以查看 "支持的 Unified Manager CLI 命令" 了解如何使用 Unified Manager CLI 添加集群。
    - 如果为集群启用了基于证书的身份验证，并且您从服务器获取 Unified Manager 的备份并还原到主机名或 IP 地址已更改的另一台 Unified Manager 服务器，则对集群的监控可能会失败。为避免失败，请编辑并保存集群详细信息。有关编辑集群详细信息的更多信息，请参见 "编辑集群"。
    - 在集群级别，Active IQ 界面为身份验证方法“cert”添加了两个新的用户组条目。

+

集群证书：此证书归 ONTAP 所有。您无法将证书已过期的集群添加到 Unified Manager，如果证书已过期，则应在添加集群之前重新生成该证书。有关证书生成的信息，请参见知识库（KB）文章 "如何在 System Manager 用户界面中续订 ONTAP 自签名证书"。

- Unified Manager 的单个实例可以支持特定数量的节点。如果需要监控超过支持节点数的环境，则必须安装额外的 Unified Manager 实例来监控部分集群。要查看支持的节点数列表，请参见 "《Unified Manager 最佳实践指南》"。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 集群设置。
2. 在“集群设置”页面上，单击*添加*。
3. 在 Add Cluster 对话框中，根据需要指定值，然后单击 **Submit**。
4. 在 Authorize Host 对话框中，单击 **View Certificate** 可查看集群的证书信息。
5. 单击 **Yes**。

   保存集群详细信息后，可以查看集群的 Mutual TLS 通信证书。

   如果未启用基于证书的身份验证，Unified Manager 仅在最初添加集群时检查证书。Unified Manager 不会检查对 ONTAP 的每次 API 调用的证书。

发现新集群的所有对象后，Unified Manager 将开始收集前 15 天的历史性能数据。这些统计数据通过数据连续性收集功能进行收集。此功能可在集群添加后立即为您提供超过两周的集群性能信息。数据连续性收集周期完成后，将默认每五分钟收集一次实时集群性能数据。

- 收集 15 天的性能数据属于 CPU 密集型操作。NetApp 建议您错开添加新集群的时间，以便数据连续性收集轮询不会同时在太多集群上运行。此外，如果您在数据连续性收集期间重新启动 Unified Manager，则收集将停止，并且您将在性能图表中看到缺失时间段的数据空白。
- 当您添加 9.14.1 或更高版本的 ONTAP 集群时，通信将通过云代理功能进行。ONTAP 会自动创建一个具有只读权限的内部服务帐户用户（例如，clus-agent-xxxx）。如果删除了该 `clus-agent`用户，Unified Manager 将停止从这些集群收集数据。

如果您收到一条错误消息，指出您无法添加集群，请查看是否存在以下问题：

- 如果两个系统上的时钟未同步且 Unified Manager HTTPS 证书开始日期晚于集群上的日期。您必须确保时钟使用 NTP 或类似服务进行同步。
- 如果集群已达到 EMS 通知目标的最大数量，则无法添加 Unified Manager 地址。默认情况下，只能在集群上定义 20 个 EMS 通知目标。

相关信息

"添加用户"

"查看集群列表和详细信息"

"安装 CA 签名并返回的 HTTPS 证书"

在 **Active IQ Unified Manager** 中编辑集群设置

您可以使用“编辑集群”对话框修改现有集群的设置，例如主机名或 IP 地址、用户名、密码和端口。

开始之前

您必须具有应用程序管理员角色或存储管理员角色。

从 Unified Manager 9.7 开始，只能使用 HTTPS 添加群集。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 集群设置。
2. 在*集群设置*页面上，选择要编辑的集群，然后单击*编辑*。
3. 在 编辑集群 对话框中，根据需要修改值。+ 如果您已修改添加到 Unified Manager 的集群的详细信息，则可以根据 ONTAP 版本查看双向 TLS 通信的证书详细信息。有关 ONTAP 版本的详细信息，请参阅 "用于相互 TLS 通信的证书"。+ 您可以通过单击 证书详细信息 查看证书详细信息。如果证书已过期，请单击 重新生成按钮以整合新证书。
4. 单击*提交*。
5. 在 Authorize Host 对话框中，单击 **View Certificate** 可查看集群的证书信息。
6. 单击 **Yes**。

相关信息

"添加用户"

"查看集群列表和详细信息"

从 **Active IQ Unified Manager** 中删除集群

您可以使用“群集设置”页面从 Unified Manager 中删除群集。例如，如果群集发现失败或要停用存储系统，则可以删除群集。

开始之前

您必须具有应用程序管理员角色或存储管理员角色。

此任务从 Unified Manager 中删除选定的集群。删除集群后，不再对其进行监控。在已删除的集群中注册的 Unified Manager 实例也将从集群中注销。

删除集群还会从 Unified Manager 中删除其所有存储对象、历史数据、存储服务以及所有关联事件。这些更改会在下一个数据收集周期后反映在清单页面和详细信息页面上。

您必须先从 Unified Manager 中删除集群，然后才能将其停用。如果尝试删除集群时该集群已处于脱机状态或无法访问，则 Unified Manager 无法与该集群通信以删除应用程序记录和已配置的事件管理系统 (EMS) 订阅。这将导致删除过程失败或在完成前无响应。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 集群设置。
2. 在“集群设置”页面上，选择要删除的集群，然后单击*删除*。
3. 在*移除数据源*消息对话框中，单击*移除*以确认移除请求。

相关信息

"添加用户"

"查看集群列表和详细信息"

在 **Active IQ Unified Manager** 中重新发现集群

您可以从“集群设置”页面手动重新发现集群，以获取有关集群运行状况、监视状态和性能状态的最新信息。

当您想要更新集群（例如在空间不足时增加聚合的大小）并且希望 Unified Manager 发现您所做的更改时，您可以手动重新发现集群。

当 Unified Manager 与 OnCommand Workflow Automation (WFA) 配对时，该配对会触发 WFA 所缓存数据的重新获取。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 集群设置。
2. 在*集群设置*页面上，单击*重新发现*。

   Unified Manager 重新发现选定集群并显示最新的运行状况和性能状态。

相关信息

"查看集群列表和详细信息"

监控 **VMware** 虚拟基础架构

了解 **Active IQ Unified Manager** 如何监控 **VMware** 虚拟基础架构

Active IQ Unified Manager 提供了对虚拟基础架构中虚拟机（VM）的可见性，并支持对虚拟环境中的存储和性能问题进行监控和故障排除。您可以使用此功能来确定存储环境中的任何延迟问题，或者 vCenter 服务器上是否存在报告的性能事件。

ONTAP 上的典型虚拟基础架构部署具有分布在计算、网络和存储层中的各种组件。VM 应用程序中的任何性能滞后都可能是由于各个层中各种组件所面临的延迟组合而发生的。此功能对存储和 vCenter Server 管理员以及 IT 通才非常有用，他们需要分析虚拟环境中的性能问题并了解问题发生在哪个组件中。

您现在可以从 VMware 部分的 vCenter 菜单访问 vCenter Server。列出的每个虚拟机的 peek 视图在 TOPOLOGY VIEW 中具有 **VCENTER SERVER** 链接，该链接可在新浏览器中启动 vCenter Server。您还可以使用 展开拓扑 按钮启动 vCenter Server，然后单击 在 **vCenter** 中查看 按钮以查看 vCenter Server 中的数据存储。

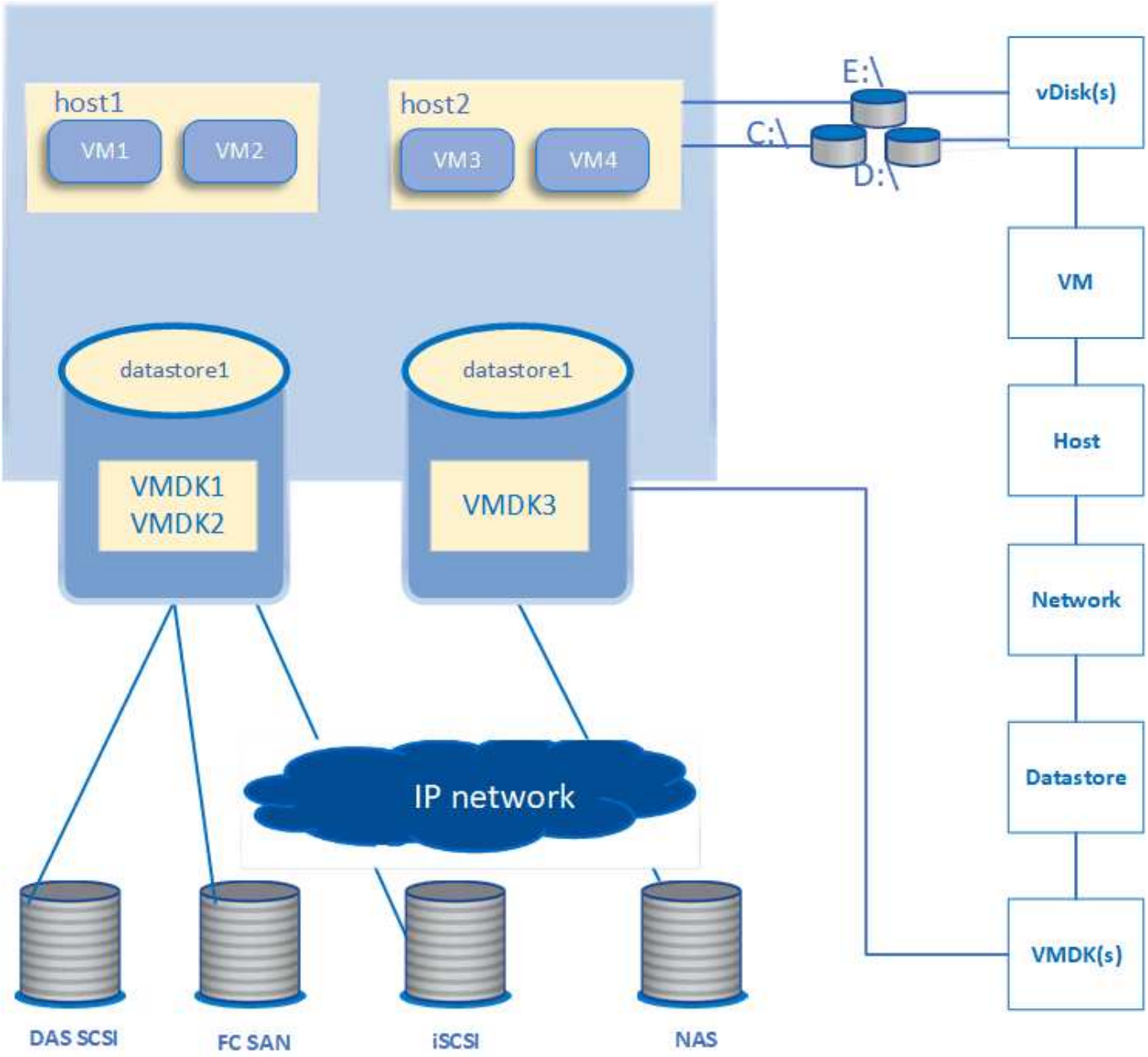
Unified Manager 以拓扑视图呈现虚拟环境的基础子系统，以确定计算节点、网络或存储中是否出现延迟问题。该视图还突出显示了导致性能滞后的特定对象，以便采取补救措施并解决根本问题。

部署在 ONTAP 存储上的虚拟基础架构包括以下对象：

- vCenter 服务器：用于管理虚拟环境中的 VMware 虚拟机、ESXi 主机和所有相关组件的集中式控制平面。有关 vCenter 服务器的详细信息，请参见 VMware 文档。
- 主机：运行 ESXi（VMware 提供的虚拟化软件）并托管虚拟机的物理或虚拟系统。
- 数据存储：数据存储是连接到 ESXi 主机的虚拟存储对象。数据存储是 ONTAP 的可管理存储实体，例如 LUN 或卷，用作 VM 文件的存储库，例如日志文件、脚本、配置文件和虚拟磁盘。它们通过 SAN 或 IP 网络连接连接到环境中的主机。映射到 vCenter Server 的 ONTAP 外部的数据存储不受支持，也不会在 Unified Manager 中显示。
- 虚拟机：VMware 虚拟机。
- 虚拟磁盘：属于具有 VMDK 扩展名的虚拟机的数据存储上的虚拟磁盘。来自虚拟磁盘的数据存储在相应的 VMDK 上。
- VMDK：数据存储库上为虚拟磁盘提供存储空间的虚拟机磁盘。每个虚拟磁盘都有一个相应的 VMDK。

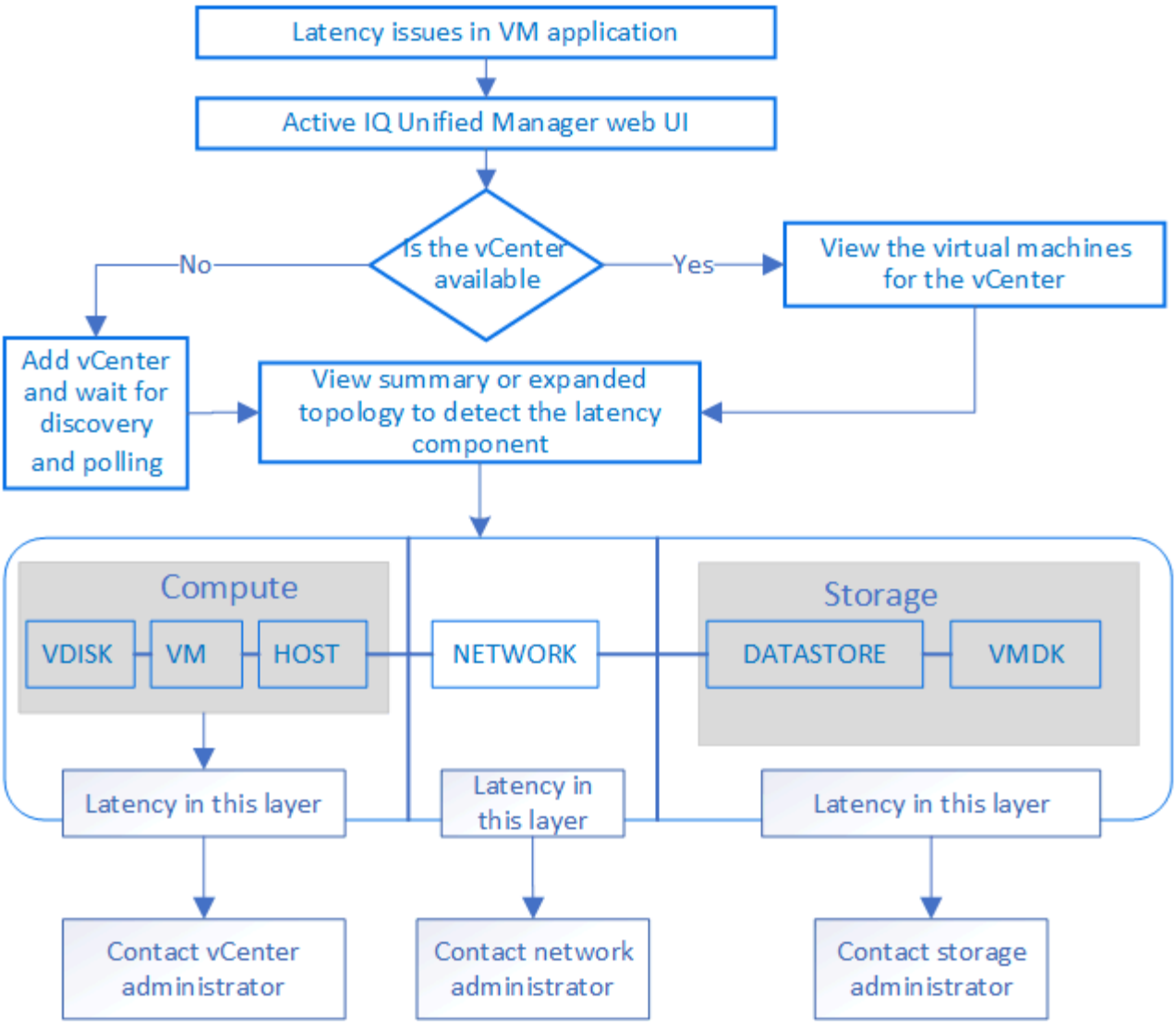
上述对象会呈现为一个虚拟机拓扑视图。

基于 **ONTAP** 的 **VMware** 虚拟化



用户工作流

下图显示了使用虚拟机拓扑视图的一个典型用例：



不支持的内容

- Unified Manager 不支持位于 ONTAP 外部且映射到 vCenter Server 实例的数据存储。同样也不支持在这些数据存储上具有虚拟磁盘的任何虚拟机。
- 不支持跨多个 LUN 的数据存储。
- 不支持使用网络地址转换（NAT）来映射数据 LIF（访问端点）的数据存储。
- 不支持在多 LIF 配置中具有相同 IP 地址的不同集群上将卷或 LUN 导出为数据存储，因为 Unified Manager 无法识别哪个数据存储属于哪个集群。

  示例：假设集群 A 具有数据存储 A。数据存储 A 通过具有相同 IP 地址 x.x.x.x 的数据 LIF 导出，并在此数据存储上创建虚拟机 A。同样，集群 B 具有数据存储 B。数据存储 B 通过具有相同 IP 地址 x.x.x.x 的数据 LIF 导出，并在数据存储 B 上创建虚拟机 B。UM 将无法将虚拟机 A 拓扑的数据存储 A 映射到相应的 ONTAP 卷/LUN，也无法映射虚拟机 B。

- 仅支持 NAS 和 SAN 卷（VMFS 的 iSCSI 和 FCP）作为数据存储，不支持虚拟卷（vVols）。
- 仅支持 iSCSI 虚拟磁盘。不支持 NVMe 和 SATA 类型的虚拟磁盘。
- 视图不允许生成用于分析各种组件性能的报告。

- 对于仅支持 Unified Manager 上的虚拟基础架构的存储虚拟机（storage VM）灾难恢复（DR）设置，必须在 vCenter Server 中手动更改配置，以便在切换和回切方案中指向活动 LUN。如果没有人工干预，其数据存储将无法访问。

在 **Active IQ Unified Manager** 中查看和添加 **vCenter Servers**

要查看虚拟机（VM）的性能并进行故障排除，必须在您的 Active IQ Unified Manager 实例上添加关联的 vCenter Server。

开始之前

在添加或查看 vCenter 服务器之前，请确保执行以下操作：

- 您知道 vCenter 服务器名称。
- 您知道 vCenter Server 的 IP 地址并拥有所需的凭据。凭据必须是 vCenter Server 管理员或对 vCenter Server 具有只读访问权限的 root 用户。
- 您要添加的 vCenter Server 运行 vSphere 6.5 或更高版本。

  适用于 VMware ESXi 和 vCenter Server 的 Unified Manager 支持提供英语和日语版本。

- vCenter Server 中的数据收集设置已设置为统计级别 *Level 3*，以确保为所有受监控对象收集所需级别的指标。间隔时间应为 *5 minutes*，保存期限应为 *1 day*。

  有关详细信息，请参见 VMware 文档中 *vSphere Monitoring and Performance Guide* 的“Data Collection Levels”部分。

- vCenter Server 中的延迟值以毫秒为单位配置，而不是以微秒为单位配置，以便成功计算延迟值。
- 将数据存储添加到 vCenter Server 时，您可以使用主机的 IP 地址或完全限定域名（FQDN）。如果要添加 FQDN，请确保 Unified Manager 服务器可以解析该域名。例如，对于 Linux 安装，请确保在 `/etc/resolv.conf` 文件中添加了域名。
- vCenter 服务器的当前时间与 vCenter 服务器时区同步。
- vCenter Server 可访问，以便成功发现。
- 将 vCenter Server 添加到 Unified Manager 时，您具有对 VMware SDK 的读取权限。这是配置轮询所必需的。

对于添加和发现的每个 vCenter 服务器，Unified Manager 都会收集配置数据，例如 vCenter 服务器和 ESXi 服务器详细信息、ONTAP 映射、数据存储区详细信息以及托管的 VM 数量。它还收集组件的性能指标。

步骤

1. 转到 **VMWARE** > **vCenter**，检查您的 vCenter Server 是否在列表中可用。

   如果您的 vCenter 服务器不可用，则必须添加 vCenter 服务器。

   a. 单击 **Add**。
   b. 为 vCenter Server 添加正确的 IP 地址，并确保设备可访问。
   c. 添加对 vCenter Server 具有只读访问权限的管理员或 root 用户的用户名和密码。

d. 如果您使用默认 443 以外的任何端口，请添加自定义端口号。

e. 单击 **Save**。

成功发现后，系统将显示一个服务器证书，您可以接受此证书。

接受证书时，vCenter 服务器将添加到可用 vCenter 服务器列表中。添加设备不会导致对关联的虚拟机进行数据收集，收集将在计划的时间间隔进行。

2. 如果您的 vCenter Server 在 **vCenters** 页面上可用，请将鼠标悬停在 状态 字段上以检查其状态，从而显示您的 vCenter Server 是否按预期运行，或者是否存在警告或错误。

添加 vCenter Server 可让您查看以下状态。但是，在添加 vCenter Server 后，相应虚拟机的性能和延迟数据可能需要长达一小时才能准确反映。

- 绿色：“正常”，表示已发现 vCenter 服务器，已成功收集性能指标
- 黄色：“警告”（例如，当 vCenter 服务器的统计级别未设置为 3 或更高以获取每个对象的统计信息时）
- 橙色：“错误”（表示任何内部错误，例如异常、配置数据收集失败或无法访问 vCenter 服务器）您可以单击列显示图标（显示/隐藏）以查看 vCenter 服务器状态的状态消息并排除故障。

3. 如果无法访问 vCenter 服务器或凭据已更改，请通过选择 **vCenter** > 编辑 来编辑 vCenter 服务器详细信息。
4. 在*编辑 VMware vCenter 服务器*页面上进行必要的更改。
5. 单击 **Save**。

vCenter Server 数据收集开始

vCenter Server 收集实时的 20 秒性能数据样本，并将其汇总为 5 分钟样本。Unified Manager 的性能数据收集计划基于 vCenter Server 的默认设置。Unified Manager 处理从 vCenter Server 获取的 5 分钟样本，并计算虚拟磁盘、虚拟机和主机的 IOPS 和延迟的每小时平均值。对于数据存储，Unified Manager 根据从 ONTAP 获取的样本计算 IOPS 和延迟的每小时平均值。这些值在整点时可用。添加 vCenter Server 后，性能指标不会立即可用，只有在下一个小时开始时才可用。在完成一个配置数据收集周期后，性能数据轮询即会开始。

对于轮询 vCenter Server 配置数据，Unified Manager 遵循与收集集群配置数据相同的计划。有关 vCenter Server 配置和性能数据收集计划的信息，请参见“集群配置和性能数据收集活动”。

相关信息

"集群配置和性能数据收集活动"

从 **Active IQ Unified Manager** 中删除 **vCenter Server**

您可以从 Active IQ Unified Manager 实例中删除 vCenter 服务器。例如，如果 vCenter 服务器发现失败或不再需要该服务器，您可以删除 vCenter 服务器。

删除 vCenter 服务器还会删除该 vCenter 上托管的所有虚拟机（VM）及其配置数据。删除 vCenter 服务器后，它及其关联的对象和历史数据将不再受监控。这些更改将反映在 vCenter 和虚拟机清单页面上。

开始之前

在删除 vCenter 服务器之前，请确保满足以下条件：

- 您具有应用程序管理员角色或存储管理员角色。
- 您应了解 vCenter 服务器名称以及与之关联的相应 IP 地址。

步骤

1. 在左侧导航窗格中，单击 **VMWARE>vCenter**。
2. 在 vCenters 页面上，选择要删除的 vCenter 服务器，然后单击 删除。
3. 在*移除 vCenter* 消息对话框中，单击*确定*以确认移除请求。

了解 **Active IQ Unified Manager** 如何监控虚拟机

对于虚拟机 (VM) 应用程序上的任何延迟问题，您可能需要监控 VM 以分析和排除原因。当其 vCenter Server 和托管 VM 存储的 ONTAP 集群添加到 Unified Manager 时，VM 即可用。

您可以在 **VMWARE** > > 虚拟机 页面上查看虚拟机的详细信息。将显示可用性、状态、已用和已分配容量、网络延迟，以及虚拟机、数据存储和主机的 IOPS 和延迟等信息。对于支持多个数据存储的虚拟机，网格会显示延迟最差的数据存储的指标，并使用星号图标（*）表示其他数据存储。如果单击该图标，则会显示其他数据存储的指标。其中一些列不可用于排序和筛选。

要查看虚拟机及其详细信息，必须完成 ONTAP 集群的发现（轮询或指标收集）。如果从 Unified Manager 中删除此集群，则在下一个发现周期之后，此虚拟机将不再可用。

在此页面中，您还可以查看虚拟机的详细拓扑，显示与虚拟机相关的组件，例如与其连接的主机、虚拟磁盘和数据存储。拓扑视图按以下顺序显示其特定层中的底层组件：虚拟磁盘 > 虚拟机 > 主机 > 网络 > 数据存储 > **VMDK**。

您可以从拓扑的角度确定 I/O 路径和组件级别延迟问题，并确定此性能问题是否是由于存储而造成的。此拓扑的摘要视图会显示此 I/O 路径，并突出显示存在 IOPS 和延迟问题的组件，以便于您确定故障排除步骤。此外，您还可以通过扩展拓扑视图单独查看各个组件以及此组件的延迟。您可以选择一个组件来确定经过各个层的 I/O 路径。

查看摘要拓扑

要通过在摘要拓扑中查看 VM 来确定性能问题，请执行以下操作：

1. 转至 **VMWARE** > **Virtual Machines**。
2. 在搜索框中输入虚拟机名称以搜索您的虚拟机。您也可以通过单击 **Filter** 按钮，根据特定条件筛选搜索结果。但是，如果找不到您的虚拟机，请确保已添加并发现相应的 vCenter Server。

   vCenter Server 允许在 vSphere 实体（例如 VM、集群、数据存储、文件夹或文件）的名称中使用特殊字符（例如 %、&、、**$**、**#**、**@**、**!**、\、**/**、:、、?、"、、<，>、|、;、'）。`VMware vCenter Server` 和 `ESX/ESXi Server` 不会转义显示名称中使用的特殊字符。但是，在 `Unified Manager` 中处理该名称时，其显示方式会有所不同。例如，在 `vCenter Server` 中名为 `` `%$VC_AIQUM_clone_191124% `` 的 VM 在 Unified Manager 中将显示为 `%25$VC_AIQUM_clone_191124%25`。在查询名称中包含特殊字符的 VM 时，必须注意此问题。

3. 检查 VM 的状态。VM 状态是从 vCenter Server 检索的。以下状态可用。有关这些状态的详细信息，请参见

VMware 文档。

- 正常
- 警告
- 警报
- 未监控
- 未知

4. 单击此虚拟机旁边的向下箭头以查看计算层、网络层和存储层中组件的拓扑摘要视图。存在延迟问题的节点会突出显示。摘要视图会显示延迟状况最差的组件。例如，如果一个虚拟机包含多个虚拟磁盘，则此视图将显示所有虚拟磁盘中延迟状况最差的虚拟磁盘。
5. 要分析数据存储在一段时间内的延迟和吞吐量，请单击数据存储对象图标顶部的 **Workload Analyzer** 按钮。您将转到“工作负载分析”页面，您可以在其中选择时间范围并查看数据存储的性能图表。有关工作负载分析器的详细信息，请参见_使用工作负载分析器对工作负载进行故障排除_。

查看展开的拓扑

您可以通过查看虚拟机的扩展拓扑来单独查看每个组件的详细信息。

步骤

1. 在摘要拓扑视图中，单击 展开拓扑。您可以单独查看每个组件的详细拓扑以及每个对象的延迟数值。如果一个类别中有多个节点，例如数据存储或 VMDK 中的多个节点，则延迟最差的节点将以红色突出显示。
2. 要检查特定对象的 IO 路径，请单击此对象以查看此 IO 路径以及相应的映射。例如，要查看某个虚拟磁盘的映射，请单击此虚拟磁盘以查看它与相应 VMDK 的映射，此映射会突出显示。如果这些组件存在性能滞后，您可以从 ONTAP 收集更多数据并对此问题进行故障排除。

不会报告 VMDK 的指标。在此拓扑中，只会显示 VMDK 名称，而不会显示相应指标。

相关信息

"使用工作负载分析器对工作负载进行故障排除"

使用 **Active IQ Unified Manager** 查看灾难恢复设置中的虚拟基础架构可见性

您可以查看托管在 MetroCluster 配置或存储虚拟机（storage VM）灾难恢复（SVM DR）设置中的数据存储的配置和性能指标。

在 Unified Manager 上，您可以查看 MetroCluster 配置中作为数据存储附加到 vCenter Server 的 NAS 卷或 LUN。在 MetroCluster 配置中托管的数据存储与标准环境中的数据存储在相同的拓扑视图中表示。

您还可以查看存储 VM 灾难恢复配置中映射到 vCenter Server 中的数据存储的 NAS 卷或 LUN。

查看 **MetroCluster** 配置中的数据存储

在 MetroCluster 配置中查看数据存储之前，请注意以下先决条件：

- 在切换和切回的情况下，HA 对的主集群和二级集群以及 vCenter 服务器的发现应该是完整的。
- HA 对的主集群和辅助集群以及 vCenter 服务器必须由 Unified Manager 管理。

- 必须在 ONTAP 和 vCenter Server 上完成所需的设置。有关信息，请参阅 ONTAP 和 vCenter 文档。

  "ONTAP 9 文档中心"

请按照以下步骤查看数据存储：

1. 在 **VMWARE** > 虚拟机 页面上，单击托管数据存储的虚拟机。单击 **Workload Analyzer** 或数据存储对象链接。在托管卷或 LUN 的主站点按预期运行的标准方案中，您可以查看主站点的 vServer 集群详细信息。
2. 如果发生灾难，并随后切换到辅助站点，则数据存储链接将指向辅助集群中卷或 LUN 的性能指标。这将在下一个集群和 vServer 发现（采集）周期完成之后反映出来。
3. 成功切回后，数据存储区链接将再次反映主集群中卷或 LUN 的性能指标。这将在下一个集群和 vServer 发现周期完成后反映出来。

在 **Storage VM** 灾难恢复配置中查看数据存储

在查看 storage VM 灾难恢复配置中的数据存储之前，请注意以下先决条件：

- 在切换和切回的情况下，HA 对的主集群和二级集群以及 vCenter 服务器的发现应该是完整的。
- 源和目标集群以及存储 VM 对等方都应由 Unified Manager 管理。
- 必须在 ONTAP 和 vCenter Server 上完成所需的设置。
  - 对于 NAS（NFS 和 VMFS）数据存储，在发生灾难时，步骤包括启动辅助存储虚拟机，验证数据 LIF 和路由，在 vCenter Server 上建立丢失的连接，以及启动虚拟机。

    对于切换回主站点，应在主站点开始提供数据之前同步卷之间的数据。

  - 对于 SAN（iSCSI 和 FC for VMFS）数据存储，vCenter Server 会将挂载的 LUN 格式化为 VMFS 格式。在发生灾难时，步骤包括启动二级存储 VM，验证数据 LIF 和路由。如果 iSCSI 目标 IP 与主 LIF 不同，则需要手动添加它们。新 LUN 应作为主机存储适配器的 iSCSI 适配器下的设备可用。此后，应使用新 LUN 创建新的 VMFS 数据存储，并使用新名称注册旧 VM。VM 必须已启动并正在运行。

    在恢复的情况下，应同步卷之间的数据。应再次使用 LUN 创建新的 VMFS 数据存储，并以新名称注册旧 VM。

    有关设置的信息，请参见 ONTAP 和 vCenter Server 文档。

  "ONTAP 9 文档中心"

请按照以下步骤查看数据存储：

1. 在 **VMWARE** > *虚拟机*页面上，单击托管数据存储的虚拟机清单。单击数据存储对象链接。在标准方案中，您可以查看主存储虚拟机中卷和 LUN 的性能数据。
2. 如果发生灾难，并随后切换到辅助存储 VM，则数据存储链接将指向辅助存储 VM 中卷或 LUN 的性能指标。在下一个集群和 vServer 发现（采集）周期完成之后，这将会反映出来。
3. 成功切回后，数据存储链接再次反映主存储 VM 中卷或 LUN 的性能指标。这会在下一个集群和 vServer 发现周期完成后反映出来。

不支持的场景

- 对于 MetroCluster 配置，请注意以下限制：

- 仅占用处于 `NORMAL`和 `SWITCHOVER`状态的集群。不支持其他状态，例如 `PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK`和 `NOT_REACHABLE`。
- 除非启用自动切换 (ASO)，否则如果主集群发生故障，则无法发现辅助集群，并且拓扑继续指向主集群中的卷或 LUN。

- 对于 storage VM 灾难恢复配置，请注意以下限制：
  - 不支持为 SAN 存储环境启用 Site Recovery Manager (SRM) 或 Storage Replication Adapter (SRA) 的配置。

配置和管理工作负载

在 **Active IQ Unified Manager** 中配置和管理工作负载

Active IQ Unified Manager 的主动管理功能提供性能服务级别、存储效率策略和存储提供商 API，用于配置、监控和管理数据中心中的存储工作负载。

默认情况下，Unified Manager 提供此功能。如果您不打算使用此功能，可以从 存储管理 > 功能设置 中将其禁用。

启用后，您可以在由 Unified Manager 实例管理的 ONTAP 集群上配置工作负载。您还可以为工作负载分配策略，例如性能服务级别和存储效率策略，并根据这些策略管理存储环境。

此功能可启用以下功能：

- 在添加的集群上自动发现存储工作负载，从而轻松评估和部署存储工作负载
- 调配支持 NFS 和 CIFS 协议的 NAS 工作负载
- 调配支持 iSCSI 和 FCP 协议的 SAN 工作负载
- 在同一文件共享上支持 NFS 和 CIFS 协议
- 性能服务级别和存储效率策略的管理
- 为存储工作负载分配性能服务级别和存储效率策略

UI 左侧窗格中的 **Provisioning**、**Storage** > **Workloads** 和 **Policies** 选项可让您修改各种配置。

您可以通过使用这些选项执行以下功能：

- 在*存储* > *工作负载*页面上查看存储工作负载
- 从"配置工作负载"页面创建存储工作负载
- 通过策略创建和管理性能服务级别
- 从策略创建和管理存储效率策略
- 从“工作负载”页面为存储工作负载分配策略

相关信息

"基于策略的存储管理"

工作负载概述

了解 **Active IQ Unified Manager** 中的工作负载仪表板

工作负载表示存储对象（如卷或 LUN）的输入/输出（I/O）操作。存储的调配方式取决于预期的工作负载要求。只有在存储对象之间存在流量后，Active IQ Unified Manager 才会跟踪工作负载统计信息。例如，工作负载 IOPS 和延迟值在用户开始使用数据库或电子邮件应用程序后可用。

工作负载页面显示由 Unified Manager 管理的 ONTAP 群集的存储工作负载摘要。它提供了有关符合性能服务级别的存储工作负载以及不符合要求的存储工作负载的一目了然的累积信息。它还使您能够评估整个数据中心内群集的总体、可用和已用容量以及性能（IOPS）。

建议您评估不符合、不可用或不由任何性能服务级别管理的存储工作负载的数量，并采取必要措施以确保其符合性、容量使用率和 IOPS。

Workloads 页面包括以下两个部分：

- 工作负载概述：概述由 Unified Manager 管理的 ONTAP 集群上的存储工作负载数量。
- 数据中心概况：提供数据中心存储工作负载的容量和 IOPS 概况。相关数据在数据中心级别以及针对各个单独的项进行显示。

工作负载概述部分

工作负载概述部分提供了存储工作负载的累积概览信息。存储工作负载的状态将根据已分配和未分配的性能服务级别进行显示。

- 已分配：针对已分配性能服务级别的存储工作负载报告以下状态：
  - 合规：存储工作负载的性能基于分配给它们的 Performance Service Levels。如果存储工作负载处于相关 Performance Service Levels 中定义的阈值延迟范围内，则将其标记为 “conforming”。合规的工作负载以蓝色标记。
  - 不符合：在性能监控期间，如果存储工作负载延迟超过关联性能服务级别中定义的阈值延迟，则存储工作负载将被标记为 “non-conforming”。不符合要求的工作负载以橙色标记。
  - 不可用：如果存储工作负载处于脱机状态或无法访问相应的集群，则将其标记为 “unavailable”。不可用的工作负载标记为红色。
- 未分配：未分配性能服务级别的存储工作负载报告为 “unassigned”。该数字由信息图标表示。

总工作负载计数是已分配和未分配工作负载的总和。

您可以单击此部分中显示的工作负载总数，然后在“工作负载”页面上查看它们。

“按性能服务级别划分的遵从性”小节显示可用存储工作负载的总数：

- 符合每种性能服务级别
- 分配的性能服务级别与建议的性能服务级别不匹配

数据中心概述部分

数据中心概述部分以图形方式表示数据中心中所有集群的可用和已用容量以及 IOPS。通过使用此数据，您应该管理存储工作负载的容量和 IOPS。该部分还显示所有集群中存储工作负载的以下信息：

- 数据中心中所有集群的总容量、可用容量和已用容量
- 数据中心中所有集群的总 IOPS、可用 IOPS 和已用 IOPS
- 基于每个性能服务级别的可用和已用容量
- 基于每个性能服务级别的可用和已用 IOPS
- 未分配任何性能服务级别的工作负载使用的总空间和 IOPS

如何根据性能服务级别计算数据中心容量和性能

将根据集群中所有存储工作负载的总已用容量和性能来检索已用容量和 IOPS。

系统将根据节点上的预期延迟和推荐的性能服务级别来计算可用的 IOPS。它包括预期延迟小于或等于其自身预期延迟的所有性能服务级别的可用 IOPS。

系统将根据聚合上的预期延迟和推荐的性能服务级别来计算可用容量。它包括预期延迟小于或等于其自身预期延迟的所有性能服务级别的可用容量。

在 **Active IQ Unified Manager** 中查看工作负载

将群集添加到 Unified Manager 时，每个群集上的存储工作负载将被自动发现并显示在“工作负载”页面上。

只有在存储工作负载上开始 I/O 操作后，Unified Manager 才会开始分析工作负载以提供建议（建议的 PSL）。

FlexGroup 卷及其成分不包括在内。

工作负载概述

“工作负载概述”页面显示数据中心中的工作负载概述以及数据中心的空间和性能概述。

- **Workloads Overview** 面板：显示工作负载的总数以及已分配或未分配 PSL 的工作负载数。此外还会显示每个 PSL 的工作负载计数细分。单击这些计数可转至包含已筛选工作负载的 **All Workloads** 视图。您还可以查看不符合系统建议的工作负载数量，并通过单击 **Assign System-Recommended PSLs** 按钮为其分配系统建议的 PSL。
- *数据中心概述*面板：显示数据中心的可用和已用空间 (TiB) 和性能 (IOPS)。还会显示每个 PSL 下所有工作负载的可用和已用空间 (TiB) 和性能 (IOPS) 的细分。

所有工作负载视图

存储 **>** 工作负载 **>** 所有工作负载 页面列出了与 Unified Manager 管理的 ONTAP 群集关联的存储工作负载。

对于新发现的没有 I/O 操作的存储工作负载，状态为 “正在等待 I/O”。在存储工作负载上开始 I/O 操作后，Unified Manager 将开始分析，并且工作负载状态将更改为 “正在学习……”。完成分析后（在 I/O 操作开始后的 24 小时内），将显示针对存储工作负载的推荐 PSL。

该页面还使您能够将存储效率策略（SEP）和性能服务级别（PSL）分配给存储工作负载。您可以执行多项任务

：

- 添加或配置存储工作负载
- 查看和筛选工作负载列表
- 将 PSL 分配给存储工作负载
- 评估系统推荐的 PSL 并将其分配给工作负载
- 将 SEP 分配给存储工作负载

添加或调配存储工作负载

您可以将存储工作负载添加或置备到支持的 LUN（同时支持 iSCSI 和 FCP 协议）、NFS 文件共享和 SMB 共享。

步骤

1. 单击*存储 > 工作负载 > 所有工作负载 > 创建*。
2. 创建工作负载。有关信息，请参见 "配置和管理工作负载"。

查看和筛选工作负载

在“所有工作负载”屏幕上，您可以查看数据中心中的所有工作负载，或根据其 PSL 或名称搜索特定存储工作负载。您可以使用过滤器图标为搜索输入特定条件。您可以按不同的筛选条件进行搜索，例如按主机集群或存储 VM 进行搜索。*总容量*选项允许按工作负载的总容量（按 MB）进行筛选。但是，在这种情况下，返回的工作负载数量可能会有所不同，因为总容量是在字节级别进行比较的。

对于每个工作负载，将显示主机集群和存储 VM 等信息，以及分配的 PSL 和 SEP。

此页面还允许您查看工作负载的性能详细信息。您可以通过单击*选择/排序列*按钮并选择要查看的特定列来查看有关工作负载的 IOPS、容量和延迟的详细信息。“性能视图”列显示工作负载的平均 IOPS 和峰值 IOPS，您可以单击工作负载分析器图标以查看详细的 IOPS 分析。

分析工作负载的性能和容量标准

*IOPS 分析*弹出窗口中的*分析工作负载*按钮将带您进入工作负载分析页面，您可以在其中选择时间范围并查看所选工作负载的延迟、吞吐量和容量趋势。有关工作负载分析器的详细信息，请参见 "使用工作负载分析器排除工作负载故障"。

您可以通过单击 性能视图 列中的条形图图标来查看有关工作负载的性能信息，以帮助进行故障排除。要在“工作负载分析”页面上查看性能和容量图表以分析对象，请单击 分析工作负载 按钮。

有关详细信息，请参见"工作负载分析器显示哪些数据"。

在 **Active IQ Unified Manager** 中将策略分配给工作负载

您可以通过使用不同的导航选项，从“所有工作负载”页面将存储效率策略（SEP）和性能服务级别（PSL）分配给存储工作负载。

将策略分配给单个工作负载

您可以将 PSL 或 SEP 或两者都分配给单个工作负载。按照以下步骤操作：

1. 选择工作负载。
2. 单击行旁边的编辑图标，然后单击*编辑*。

   *分配的性能服务级别*和*存储效率策略*字段已启用。

3. 选择所需的 PSL 或 SEP，或两者皆选。
4. 单击复选图标以应用更改。

您还可以选择一个工作负载，然后单击*更多操作*以分配策略。

为多个存储工作负载分配策略

您可以将 PSL 或 SEP 一起分配给多个存储工作负载。请按照以下步骤操作：

1. 选中要为其分配策略的工作负载的复选框，或选择数据中心中的所有工作负载。
2. 单击*更多操作*。
3. 要分配 PSL，请选择 分配性能服务级别。要分配 SEP，请选择 分配存储效率策略。此时将显示一个弹出窗口，供您选择策略。
4. 选择适当的策略，然后单击*应用*。此时将显示已分配策略的工作负载数量。同时还会列出未分配策略的工作负载及其原因。

对批量工作负载应用策略可能需要一些时间，具体取决于所选工作负载的数量。您可以单击*在后台运行*按钮，并在操作于后台运行时继续执行其他任务。批量分配完成后，您可以查看完成状态。如果您要对多个工作负载应用 PSL，则在批量分配的上一个作业正在运行时，无法触发另一个请求。

将系统建议的 **PSL** 分配给工作负载

您可以将系统建议的 PSL 分配给数据中心中未分配 PSL 或分配的 PSL 与系统建议不匹配的存储工作负载。要使用此功能，请单击 分配系统推荐的 **PSL** 按钮。您不必选择特定的工作负载。

该建议由系统分析内部确定，对于 IOPS 和其他参数与任何可用 PSL 的定义不符的工作负载，将跳过该建议。具有 `Waiting for I/O`和学习状态的存储工作负载也被排除在外。

Unified Manager 会在工作负载名称中查找特殊关键字，以覆盖系统分析并为工作负载推荐不同的 PSL。当工作负载的名称中包含字母 “ora” 时，建议使用 **Extreme Performance**PSL。当工作负载的名称中包含字母 “vm” 时，建议使用 **Performance**PSL。

另请参阅知识库（KB）文章 "ActiveIQ Unified Manager “分配系统建议的性能服务级别”不适应高度可变的工作负载"

在 **Active IQ Unified Manager** 中配置文件共享卷

您可以从 Provision Workload 页面在现有集群和 Storage Virtual Machine （storage VM）上创建支持 CIFS/SMB 和 NFS 协议的文件共享卷。

开始之前

- 此存储 VM 必须具有配置文件共享卷的空间。
- 您的存储 VM 上应启用 SMB 和 NFS 服务之一或两者。
- 要为工作负载选择和分配性能服务级别（PSL）和存储效率策略（SEP），必须在开始创建工作负载之前创建这些策略。

步骤

1. 在 配置工作负载 页面上，添加要创建的工作负载的名称，然后从可用列表中选择集群。
2. 根据您选择的集群，**STORAGE VM** 字段会筛选该集群可用的存储 VM。从列表中选择所需的存储 VM。

   基于存储虚拟机上支持的 SMB 和 NFS 服务，在主机信息部分中启用 NAS 选项。

3. 在存储和优化部分，为工作负载分配存储容量和 PSL，以及可选的 SEP。

   SEP 的规范分配给 LUN，PSL 的定义在创建时应用于工作负载。

4. 如果要强制执行分配给工作负载的 PSL，请选中 强制执行性能限制 复选框。

   将 PSL 分配给工作负载可确保创建工作负载的聚合可以支持相应策略中定义的性能和容量目标。例如，如果工作负载被分配了“Extreme Performance”PSL，则在其上配置工作负载的聚合应具有支持“Extreme Performance”策略的性能和容量目标的能力，例如 SSD 存储。

   除非选中此复选框，否则 PSL 不会应用于工作负载，并且仪表板上工作负载的状态将显示为未分配。

5. 选择 **NAS** 选项。

   如果看不到启用的 **NAS** 选项，请验证选定的存储 VM 是否支持 SMB 或 NFS，或者两者都支持。

   如果您的存储 VM 同时启用了 SMB 和 NFS 服务，则可以选中 通过 **NFS** 共享 和 通过 **SMB** 共享 复选框，并创建同时支持 NFS 和 SMB 协议的文件共享。如果要创建 SMB 或 CIFS 共享，请仅选中相应的复选框。

6. 对于 NFS 文件共享卷，指定要访问文件共享卷的主机或网络的 IP 地址。您可以为多台主机输入以逗号分隔的值。

   在添加主机 IP 地址时，将运行内部检查，以将主机详细信息与存储 VM 匹配，并创建该主机的导出策略，或者如果存在现有策略，则重用该策略。如果为同一主机创建了多个 NFS 共享，则对所有文件共享重复使用具有匹配规则的同一主机的可用导出策略。使用 API 配置 NFS 共享时，可以使用通过提供特定策略密钥来指定单个策略的规则或重用策略的功能。

7. 对于 SMB 共享，请指定可访问此 SMB 共享的用户或用户组，并分配所需权限。对于每组用户，在创建文件共享期间会生成一个新的访问控制列表 (Access Control List, ACL)。
8. 单击 **Save**。

   此时，此工作负载将添加到存储工作负载列表中。

在 **Active IQ Unified Manager** 中配置 **LUN**

您可以从 Provision Workload 页面在现有集群和 Storage Virtual Machine （storage VM）

上创建支持 CIFS/SMB 和 NFS 协议的 LUN。

开始之前

- 此存储 VM 必须具有调配此 LUN 的空间。
- 必须在创建 LUN 的存储 VM 上同时启用 iSCSI 和 FCP。
- 要为工作负载选择和分配性能服务级别（PSL）和存储效率策略（SEP），必须在开始创建工作负载之前创建这些策略。

步骤

1. 在 配置工作负载 页面上，添加要创建的工作负载的名称，然后从可用列表中选择集群。

   根据您选择的集群，**STORAGE VM** 字段会筛选该集群可用的存储虚拟机。

2. 从列表中选择支持 iSCSI 和 FCP 服务的 Storage VM。

   根据您的选择，系统会在主机信息部分中启用 SAN 选项。

3. 在*存储和优化*部分，为工作负载分配存储容量和 PSL，以及可选的 SEP。

   SEP 的规范分配给 LUN，PSL 的定义在创建时应用于工作负载。

4. 如果要在工作负载上强制执行分配的 PSL，请选中*强制执行性能限制*复选框。

   将 PSL 分配给工作负载可确保创建工作负载的聚合能够支持相应策略中定义的性能和容量目标。例如，如果为工作负载分配了“极限性能”PSL，则要配置该工作负载的聚合应具备支持“极限性能”策略的性能和容量目标的能力，例如 SSD 存储。

   除非选中此复选框，否则 PSL 不会应用于工作负载，并且仪表板上工作负载的状态将显示为 `unassigned`。

5. 选择 **SAN** 选项。如果未看到启用的 **SAN** 选项，请验证选定的存储虚拟机是否支持 iSCSI 和 FCP。
6. 选择主机操作系统。
7. 指定主机映射以控制启动程序对 LUN 的访问。您可以分配现有的启动程序组（igroup），或定义和映射新的 igroup。

   如果在调配 LUN 时创建新的 igroup，则需要等到下一个发现周期（最多 15 分钟）才能使用它。因此，建议您使用可用 igroup 列表中的现有 igroup。

   如果要创建新的 igroup，请选择*创建新的启动程序组*按钮，然后输入 igroup 的信息。

8. 单击 **Save**。

   该 LUN 已添加到存储工作负载列表中。

管理性能服务级别

性能服务级别（PSL）使您能够定义工作负载的性能和存储目标。您可以在最初创建工作负载时或之后通过编辑工作负载，为工作负载分配 PSL。

存储资源的管理和监控基于服务级别目标（SLO）。SLO 由基于所需性能和容量的服务级别协议定义。在 Unified Manager 中，SLO 是指在 NetApp 存储上运行的应用程序的 PSL 定义。存储服务根据底层资源的性能和利用率进行区分。PSL 是存储服务目标的描述。PSL 使存储提供商能够为工作负载指定性能和容量目标。当您在工作负载上分配 PSL 时，ONTAP 上的相应工作负载将由其性能和容量目标进行管理。每个 PSL 都由峰值、预期和绝对最小 IOPs 以及预期延迟控制。

Unified Manager 具有以下类型的 PSL：

- 系统定义：Unified Manager 提供了一些无法更改的预设策略。这些预定义的 PSL 是：
  - 至高性能
  - 性能
  - 值

  Extreme Performance、Performance 和 Value PSL 适用于数据中心的大多数常见存储工作负载。

  Unified Manager 还为数据库应用程序提供三个性能服务级别。这些是支持突发 IOPS 的极高性能 PSL，适用于具有最高吞吐量需求的数据库应用程序。
  - 数据库日志的 Extreme
  - Extreme for Database Shared Data
  - 数据库数据的 Extreme
- 用户自定义：如果预定义的性能服务级别不满足您的需求，您可以创建新的 PSL 来满足您的需求。有关信息，请参见 "创建和编辑性能服务级别"。
- **Beyond Extreme**：Beyond Extreme PSL 是系统推荐的 PSL，建议用于要求 IOPs 高于 Extreme 的工作负载。系统会根据这些工作负载的 IOPS、容量和延迟对其进行内部分析，并在 存储 **>** 工作负载 **>** 所有工作负载 屏幕上为每个工作负载推荐 Beyond Extreme PSL。您可以将 PSL 应用于工作负载，以确保获得最佳性能。

  工作负载的 IOPs 参数是动态生成的，具体取决于工作负载行为，并以 `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`的格式附加到 `Beyond Extreme PSL` 的名称后。例如，如果系统确定工作负载的峰值和预期 `IOPs` 分别为 `106345`和 `37929`，则为该工作负载生成的 Beyond Extreme PSL 将命名为 `Beyond Extreme 106345 37929`。虽然这些 PSL 是系统推荐的，但当您将它们分配给工作负载时，这些 PSL 的类型会被标记为 `User-defined`。

通过分配 **PSL** 管理工作负载

您可以从 策略 > 性能服务级别 页面并使用存储提供商 API 访问 PSL。通过向存储工作负载分配 PSL 来管理存储工作负载非常方便，因为您不必单独管理存储工作负载。任何修改也可以通过重新分配另一个 PSL 来管理，而不是单独管理它们。Unified Manager 可帮助您根据内部评估和建议为工作负载分配 PSL。

有关将系统推荐的 PSL 分配给工作负载的信息，请参见 "将系统建议的 PSL 分配给工作负载"

性能服务级别页面列出了可用的 PSL 策略，并允许您添加、编辑和删除它们。

您无法修改系统定义的或当前分配给工作负载的 PSL。无法删除分配给工作负载的 PSL，如果它是唯一可用的 PSL，也无法删除。

此页面显示以下信息：

字段	问题描述
名称	PSL 的名称。
类型	此策略是系统定义的还是用户定义的。
预期 IOPS/TB	应用程序预期在 LUN 或文件共享上执行的最小 IOPS 数。预期 IOPS 根据已分配的存储对象大小指定已分配的最低预期 IOPS。
峰值 IOPS/TB	应用程序可在 LUN 或文件共享上执行的最大 IOPS 数。Peak IOPS 根据已分配的存储对象大小或已使用的存储对象大小指定已分配的最大可能 IOPS。 Peak IOPS 基于分配策略。分配策略为 allocated-space 或 used-space。当分配策略设置为 allocated-space 时，系统将根据存储对象的大小计算峰值 IOPS。当分配策略设置为 used-space 时，系统将根据存储对象中存储的数据量并考虑存储效率来计算峰值 IOPS。默认情况下，分配策略设置为 used-space。
绝对最小 IOPS	当预期 IOPS 小于此值时，绝对最小 IOPS 将用作覆盖。系统定义的 PSL 的默认值如下： • 极致性能：如果预期 IOPS >= 6144/TB，则绝对最小 IOPS = 1000 • 性能：如果预期 IOPS >= 2048/TB 且 < 6144/TB，则绝对最小 IOPS = 500 • 值：如果预期 IOPS >= 128/TB 且 < 2048/TB，则绝对最小 IOPS = 75 系统定义的数据库 PSL 的默认值如下： • 数据库日志的 Extreme：如果预期 IOPS >= 22528，则绝对最小 IOPS = 4000 • 数据库共享数据的 Extreme：如果预期 IOPS >= 16384，则绝对最小 IOPS = 2000 • 数据库数据的 Extreme：如果预期 IOPS >= 12288，则绝对最小 IOPS = 2000 自定义 PSL 的绝对最小 IOPS 的较高值最多可为 75000。较低的值按以下方式计算： 1000/预期延迟
预期延迟	存储 IOPS 的预期延迟，以毫秒/操作（ms/op）为单位。

字段	问题描述
容量	集群中的可用和已用容量总计。
工作负载	已分配 PSL 的存储工作负载数。

有关峰值 IOPS 和预期 IOPS 如何帮助在 ONTAP 集群上实现一致的差异化性能的信息，请参见以下知识库文章：“什么是性能预算？”

为违反 **PSL** 定义的阈值的工作负载生成的事件

请注意，如果工作负载在过去一小时内有 30% 的时间超过预期延迟值，Unified Manager 将生成以下事件之一，以通知您潜在的性能问题：

- 已违反性能服务级别策略定义的工作负载卷延迟阈值
- 已违反性能服务级别策略定义的工作负载 LUN 延迟阈值。

您可能需要分析工作负载，以了解可能导致更高延迟值的原因。

有关详细信息，请参见以下链接：

- “卷事件”
- “违反性能阈值策略时会发生什么”
- “Unified Manager 如何使用工作负载延迟来识别性能问题”
- “什么是性能事件”

系统定义的 **PSL**

下表提供了有关系统定义的 PSL 的信息：

性能服务级别	说明和用例	预期延迟（毫秒/操作）	**IOPS** 峰值	预期 **IOPS**	绝对最小 **IOPS**
至高性能	提供至高吞吐量和至低延迟 最适合延迟敏感型应用程序	1	12288	6144	1000
性能	提供高吞吐量和低延迟 非常适合数据库和虚拟化应用程序	2	4096	2048	500

性能服务级别	说明和用例	预期延迟（毫秒/操作）	IOPS 峰值	预期 IOPS	绝对最小 IOPS
值	提供高存储容量和中等延迟 非常适合高容量应用，如电子邮件、Web 内容、文件共享和备份目标	17	512	128	75
数据库日志的 Extreme	以最低延迟提供最大吞吐量。 非常适合支持数据库日志的数据库应用程序。此 PSL 提供最高的吞吐量，因为数据库日志具有极强的突发性，并且不断需要日志记录。	1	45056	22528	4000
Extreme for Database Shared Data	提供非常高的吞吐量和最低延迟。 非常适合存储在通用数据存储中但跨数据库共享的数据库应用程序数据。	1	32768	16384	2000
数据库数据的 Extreme	以最低延迟提供高吞吐量。 非常适合数据库应用程序数据，例如数据库表信息和元数据。	1	24576	12288	2000

在 **Active IQ Unified Manager** 中创建和编辑性能服务级别

当系统定义的性能服务级别与您的工作负载要求不匹配时，您可以创建自己的性能服务级别，以针对您的工作负载进行优化。

开始之前

- 您必须具有应用程序管理员角色。
- 性能服务级别名称必须是唯一的，并且不能使用以下保留关键字：

  `Prime、 Extreme、 Performance、 Value、 Unassigned、 Learning、 Idle、 Default` 和 `None`。

您可以通过定义访问存储的应用程序所需的服务级别目标，在“性能服务级别”页面中创建和编辑自定义性能服务级别。

如果性能服务级别当前已分配给工作负载，则无法对其进行修改。

步骤

1. 在*设置*下的左侧导航窗格中，选择*策略* > 性能服务级别。
2. 在*性能服务级别*页面中，根据您是要创建新的性能服务级别还是要编辑现有的性能服务级别，单击相应的按钮。

目的	按照下面的步骤进行操作……
创建新的性能服务级别	单击 **Add**。
编辑现有性能服务级别	选择一个现有的性能服务级别，然后单击*编辑*。

将显示用于添加或编辑性能服务级别的页面。

3. 通过指定性能目标自定义性能服务级别，然后单击*提交*以保存性能服务级别。

您可以从工作负载页面或在调配新工作负载时将新的或更改的性能服务级别应用于工作负载（LUN、NFS 文件共享、CIFS 共享）。

管理存储效率策略

在 **Active IQ Unified Manager** 中管理存储效率策略

存储效率策略（ SEP ）使您能够定义工作负载的存储效率特性。您可以在最初创建工作负载时将 SEP 分配给工作负载，也可以在之后通过编辑工作负载进行分配。

存储效率包括使用可提高存储利用率和降低存储成本的技术，例如精简配置、重复数据删除和数据压缩。在创建 SEP 时，您可以单独或一起使用这些节省空间的技术，以实现最大的存储效率。将策略与存储工作负载关联时，将为它们分配指定的策略设置。Unified Manager 使您能够分配系统定义和用户定义的 SEP，以优化数据中心的存储资源。

Unified Manager 提供两个系统定义的 SEP：高和低。这些 SEP 适用于数据中心中的大多数存储工作负载，但是，如果系统定义的 SEP 不满足您的要求，您可以创建自己的策略。

您无法修改系统定义的或当前分配给工作负载的 SEP。您无法删除分配给工作负载的 SEP，如果它是唯一可用的 SEP，也无法删除。

存储效率策略页面列出了可用的 SEP，并允许您添加、编辑和删除自定义的 SEP。此页面显示下列信息：

字段	问题描述
名称	SEP 的名称。
类型	此策略是系统定义的还是用户定义的。
空间预留	此卷是精简配置还是厚配置。

字段	问题描述
重复数据删除	是否在工作负载上启用重复数据删除： • 内联：在工作负载上写入时发生重复数据删除 • 背景：重复数据删除发生在工作负载中 • 禁用：在工作负载上已禁用重复数据删除
数据压缩	是否在工作负载上启用数据压缩： • 内联：在写入工作负载时发生数据压缩 • 背景：数据压缩发生在工作负载中 • 禁用：在工作负载上已禁用数据压缩
工作负载	已分配给 SEP 的存储工作负载数

创建自定义存储效率策略的准则

如果现有 SEP 不符合存储工作负载的策略要求，则可以创建自定义 SEP。但是，建议尝试对存储工作负载使用系统定义的 SEP，并且仅在必要时创建自定义 SEP。

您可以在所有工作负载页面和卷/运行状况详细信息页面中查看分配给工作负载的 SEP。您可以在仪表板的“容量”面板和“容量：所有集群”视图中查看基于这些存储效率的集群级数据缩减率（不包括 Snapshot 副本）。

在 **Active IQ Unified Manager** 中创建和编辑存储效率策略

当系统定义的存储效率策略与您的工作负载要求不匹配时，您可以创建针对您的工作负载进行优化的自己的存储效率策略。

开始之前

- 您必须具有应用程序管理员角色。
- 存储效率策略名称必须是唯一的，并且不能使用以下保留关键字：

  `High`、 `Low`、 `Unassigned`、 `Learning`、 `Idle`、 `Default` 和 `None`。

通过定义将访问存储的应用程序所需的存储效率特性，可以从存储效率策略页面创建和编辑自定义存储效率策略。

如果当前已将存储效率策略分配给工作负载，则无法对其进行修改。

步骤

1. 在左侧导航窗格的 设置 下，选择 策略 > 存储效率。
2. 在*存储效率策略*页面中，根据您是要创建新的存储效率策略还是编辑现有存储效率策略，单击相应的按钮。

目的	按照下面的步骤进行操作……
创建新的存储效率策略	点击*添加*

目的	按照下面的步骤进行操作……
编辑现有存储效率策略	选择现有存储效率策略并单击*编辑*

此时将显示添加或编辑存储效率策略的页面。

3. 通过指定存储效率特性自定义存储效率策略，然后单击*提交*以保存存储效率策略。

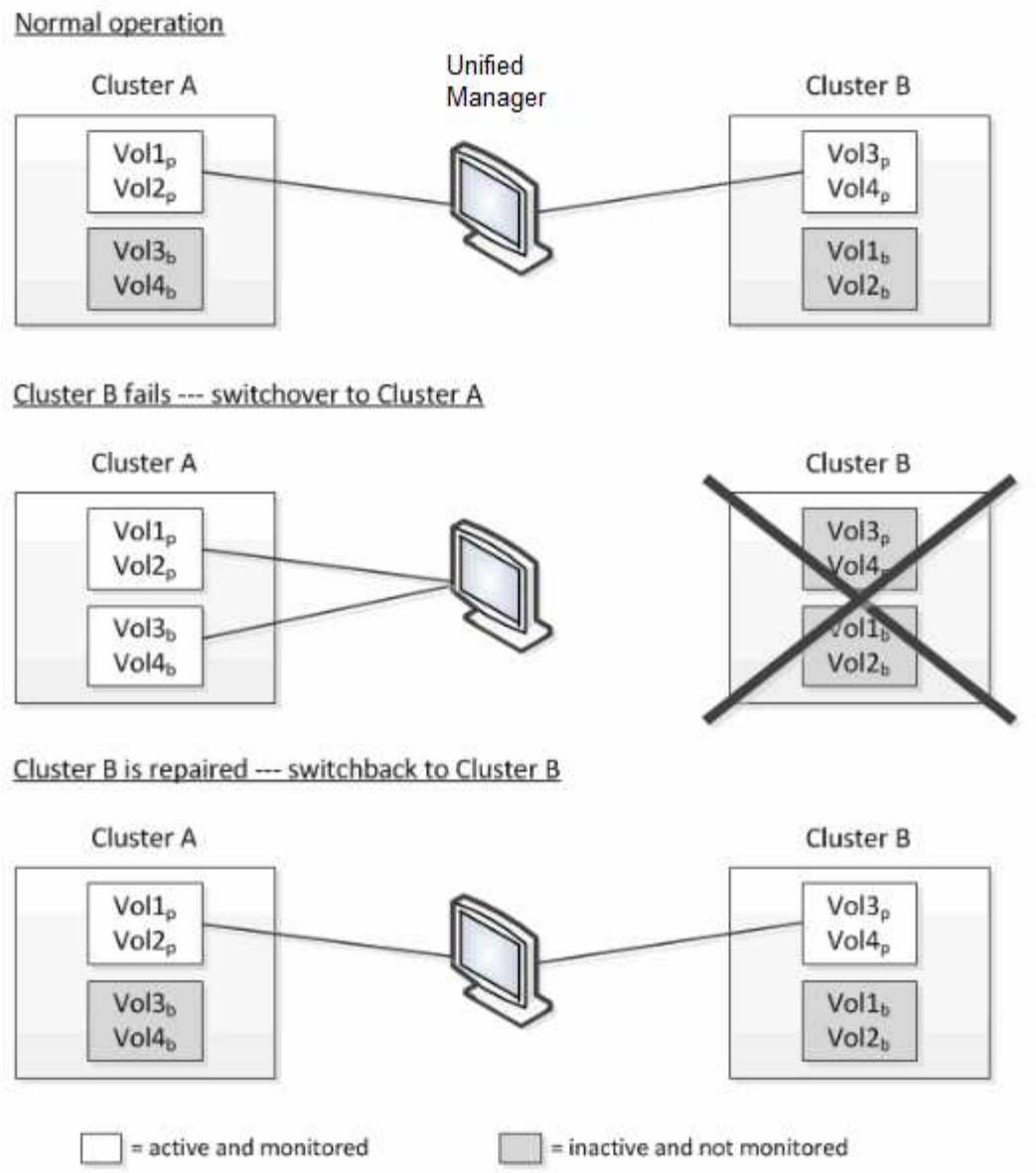
您可以从工作负载页面或在调配新工作负载时将新的或更改的存储效率策略应用于工作负载（LUN、NFS 文件共享、CIFS 共享）。

管理和监控 MetroCluster 配置

了解 Active IQ Unified Manager 中切换和切回期间的卷行为

触发切换或回切的事件会导致活动卷从灾难恢复组中的一个集群移动到另一个集群。处于活动状态并向客户端提供数据的集群上的卷将停止，而另一个集群上的卷将被激活并开始提供数据。Unified Manager 仅监控处于活动状态且正在运行的卷。

由于卷从一个群集移动到另一个群集，因此建议您监控这两个群集。Unified Manager 的单个实例可以监控 MetroCluster 配置中的两个群集，但有时两个位置之间的距离需要使用两个 Unified Manager 实例来监控这两个群集。下图显示了 Unified Manager 的单个实例：



名称中带有 p 的卷表示主卷，名称中带有 b 的卷是由 SnapMirror 创建的镜像备份卷。

正常运行期间：

- 集群 A 有两个活动卷：Vol1p 和 Vol2p。
- 集群 B 有两个活动卷：Vol3p 和 Vol4p。
- 集群 A 有两个非活动卷：Vol3b 和 Vol4b。
- 集群 B 有两个非活动卷：Vol1b 和 Vol2b。

与每个活动卷（统计信息、事件等）相关的信息由 Unified Manager 收集。集群 A 收集 Vol1p 和 Vol2p 统计数据，集群 B 收集 Vol3p 和 Vol4p 统计数据。

灾难性故障导致活动卷从集群 B 切换到集群 A 后：

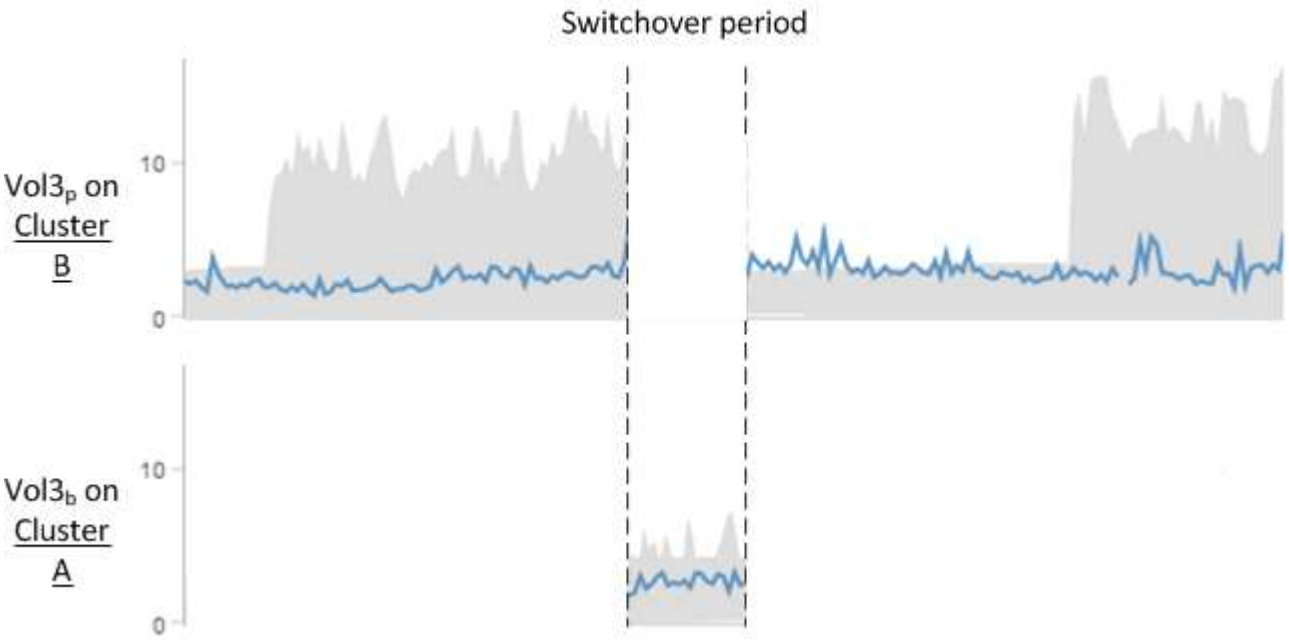
- 集群 A 有四个活动卷：Vol1p、Vol2p、Vol3b 和 Vol4b。
- 集群 B 有四个非活动卷：Vol3p、Vol4p、Vol1b 和 Vol2b。

与正常操作期间一样，与每个活动卷相关的信息由 Unified Manager 收集。但在这种情况下，Vol1p 和 Vol2p 统计数据由集群 A 收集，Vol3b 和 Vol4b 统计数据也由集群 A 收集。

请注意，Vol3p 和 Vol3b 不是相同的卷，因为它们位于不同的集群上。Unified Manager 中 Vol3p 的信息与 Vol3b 不同：

- 在切换到群集 A 期间，Vol3p 统计信息和事件不可见。
- 在第一次切换时，Vol3b 看起来像一个没有历史信息的新卷。

当集群 B 修复并执行切回时，Vol3p 在集群 B 上再次处于活动状态，并保留历史统计数据，但切换期间的统计数据会出现空白。在发生另一次切换之前，无法从集群 A 查看 Vol3b：



- 不活动的 MetroCluster 卷，例如，切回后集群 A 上的 Vol3b，将使用消息“`This volume was deleted`”进行标识。该卷实际上并未被删除，但由于它不是活动卷，因此 Unified Manager 当前未对其进行监控。
- 如果单个 Unified Manager 正在监视 MetroCluster 配置中的两个群集，则卷搜索将返回当时处于活动状态的任何卷的信息。例如，如果已发生切换并且 Vol3 在群集 A 上变为活动状态，则搜索“Vol3”将返回群集 A 上 Vol3b 的统计数据和事件。

了解 **Active IQ Unified Manager** 中基于 **FC** 的 **MetroCluster** 配置中的集群连接性

基于 FC 的 MetroCluster 配置中集群之间的连接可以为以下状态之一：最佳、受影响或关闭。了解连接状态使您能够有效地管理 MetroCluster 配置。

连接状态	问题描述	显示的图标
最佳	MetroCluster 配置中集群之间的连接正常。	

连接状态	问题描述	显示的图标
受影响	一个或多个错误会影响故障转移可用性状态；但是，MetroCluster 配置中的两个集群仍处于正常运行状态。例如，当 ISL 链路关闭、集群间 IP 链路关闭或无法访问伙伴集群时。	
已关闭	MetroCluster 配置中的集群之间的连接已断开，因为其中一个或两个集群已关闭，或者集群处于故障转移模式。例如，当配对集群因灾难而关闭时，或者出于测试目的进行计划内切换时。	切换时出错： 切换成功：

了解 **Active IQ Unified Manager** 中基于 **FC** 的 **MetroCluster** 数据镜像

MetroCluster over FC 配置提供数据镜像，以及在整个站点不可用时启动故障转移的额外功能。在 MetroCluster over FC 配置中，集群之间的数据镜像状态可以是 Normal（正常）或 Mirroring Unavailable（镜像不可用）。了解这些状态有助于您有效地管理 MetroCluster 配置。

数据镜像状态	问题描述	显示的图标
正常	MetroCluster 配置中的群集之间的数据镜像正常。	
镜像不可用	由于切换，MetroCluster 配置中的集群之间的数据镜像不可用。例如，当配对集群因灾难而停机时，或者出于测试目的进行计划内切换时。	切换时出错： 切换成功：

在 **Active IQ Unified Manager** 中监控 **MetroCluster** 配置

您可以在 MetroCluster 配置中监控连接问题。详细信息包括组件的状态和群集内的连接，

以及 MetroCluster 配置中群集之间的连接状态。在这里，您将了解如何监控受基于 FC 的 MetroCluster 和基于 IP 的 MetroCluster 配置保护的群集中的连接问题。

您可以从 Active IQ Unified Manager 左侧导航窗格中的以下视图监控 MetroCluster 配置：

- 存储 > 集群 > 保护：**MetroCluster** 视图
- 保护 > 关系 > 关系：**MetroCluster** 视图

Unified Manager 使用系统健康警报来指示 MetroCluster 配置中组件和连接的状态。

开始之前

- 必须将 MetroCluster 配置中的本地和远程集群都添加到 Active IQ Unified Manager。
- 在 MetroCluster IP 配置中，如果要支持调解器，则应配置调解器，并通过相应的 API 将其添加到集群中。
- 您必须具有操作员、应用程序管理员或存储管理员角色。

监控基于 **FC** 的 **MetroCluster** 配置中的连接问题

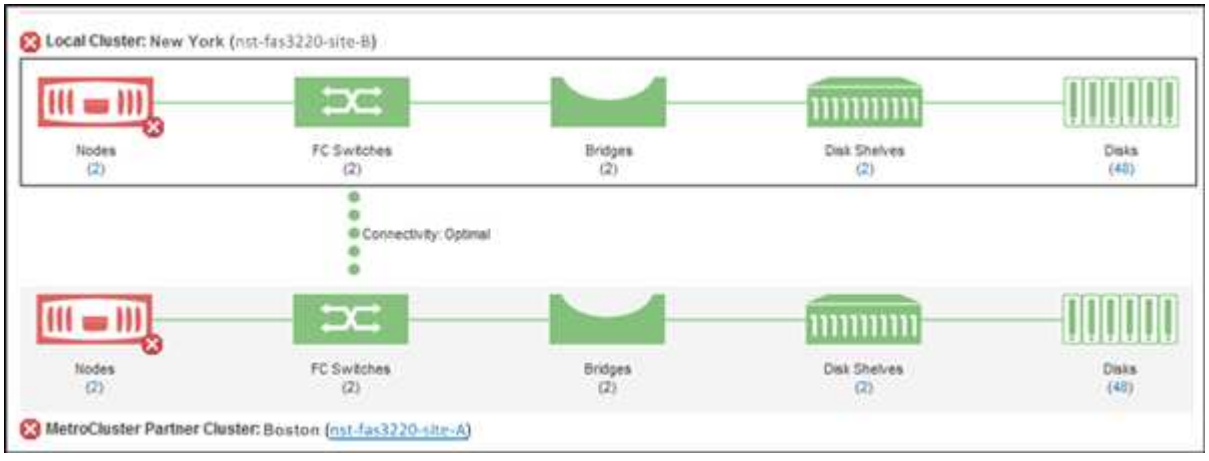
对于基于 FC 的 MetroCluster 配置中的集群，连接图表显示在 集群 / 运行状况 详细信息页面上。请按照以下步骤操作。

步骤

1. 在左侧导航窗格中，单击 存储 > 集群。

   将显示所有受监控群集的列表。

2. 在 保护：**MetroCluster** 视图中，单击要查看其 MetroCluster over FC 配置详细信息的集群的名称。或者，您可以按 MetroCluster 配置中的集群进行筛选。
3. 在*集群/健康*详细信息页面中，单击*MetroCluster 连接*选项卡。*MetroCluster 连接*选项卡仅适用于基于 FC 的 MetroCluster 配置。



MetroCluster 配置的拓扑显示在相应的集群对象区域中。您可以使用“集群/运行状况”详细信息页面中显示的信息来解决任何连接问题。例如，如果集群中节点与交换机之间的连接断开，则会显示以下图标：



如果将指针移到图标上，则可以查看有关生成的事件的详细信息。

如果在 MetroCluster 配置中发现连接问题，则必须登录到 System Manager 或访问 ONTAP CLI 以解决问题。

有关确定群集运行状况的详细信息，请参见 "确定 FC 配置中 MetroCluster 的集群运行状况"。

监控 **MetroCluster over IP** 配置中的连接问题

对于 MetroCluster over IP 配置中的集群，连接图表显示在*集群*页面上。请按照以下步骤操作。

步骤

1. 在左侧导航窗格中，单击 存储 > 集群。

   将显示所有受监控群集的列表。

2. 在*保护：MetroClusters*视图中，单击要查看其 MetroCluster over IP 配置详细信息的集群名称。或者，您可以按 MetroCluster 配置中的集群进行筛选。
3. 单击插入符号 `v`图标展开行。仅当集群受基于 IP 的 MetroCluster 配置保护时，才会显示插入符号图标。

   您可以查看源站点和镜像站点的拓扑，以及用于连接的 Mediator（如果有）。您可以查看以下信息：

   - 跨站点连接
   - 两个站点上的运行状况和可用性问题（如果有）
   - 调解器相关问题
   - 与复制相关的问题。

   报告以下状态：Critical（）、Error（）或 Normal（）。您还可以在同一拓扑中查看主数据和镜像数据的聚合数据复制状态。

   在下图中，您可以看到源和目标集群之间的站点间连接不可用，并且未配置它们之间的 Mediator。



4. 单击状态图标。将显示包含错误定义的消息。如果在您的 MetroCluster over IP 配置中针对该问题引发了事件，则可以单击消息上的 查看事件 按钮并查看事件详细信息。解决问题和事件后，此拓扑中的状态图标将变为正常（）。

5. 您可以在*集群/健康*详细信息页面的*配置*选项卡上的*MetroCluster 概述*和*保护*部分查看更多配置详细信息。

仅对于基于 IP 的 MetroCluster 配置，您可以在 集群 页面上查看集群拓扑。对于基于 FC 的 MetroCluster 配置中的集群，拓扑显示在 集群/运行状况 详细信息页面的 **MetroCluster** 连接 选项卡上。

相关信息

- "集群/运行状况详细信息页面"
- 有关 关系：**MetroCluster** 视图的信息，请参见 "监控 MetroCluster 配置"。
- 有关 关系：过去 **1** 个月的传输状态 视图的信息，请参阅 "关系：过去 1 个月的传输状态视图"。
- 有关*关系：过去 1 个月的传输速率*视图的信息，请参阅 "关系：过去 1 个月的传输速率视图"。
- 有关*关系：所有关系*视图的信息，请参见 "关系：所有关系视图"。

在 **Active IQ Unified Manager** 中监控 **MetroCluster** 复制

您可以在镜像数据的同时监控和诊断逻辑连接的整体健康状况。您可以识别中断聚合、节点和存储虚拟机等群集组件镜像的问题或任何风险。

Unified Manager 使用系统健康警报来监控 MetroCluster 配置中组件和连接的状态。

开始之前

MetroCluster 配置中的本地和远程集群都必须添加到 Unified Manager 中

查看 **MetroCluster** 跨 **IP** 配置的复制

对于 MetroCluster over IP 配置，数据复制状态将从 Unified Manager 左侧导航窗格中的以下视图显示在由 MetroCluster over IP 保护的集群的拓扑 peek 视图中：

- 存储 > 集群 > 保护：**MetroCluster** 视图
- 保护 > 关系 > 关系：**MetroCluster** 视图

有关信息，请参见 "监控 MetroCluster over IP 中的连接问题"。

查看基于 **FC** 的 **MetroCluster** 配置的复制

按照以下步骤确定基于 FC 的 MetroCluster 配置的数据复制中的任何问题。

步骤

1. 在左侧导航窗格中，单击 存储 > 集群。

   此时将显示受监控集群的列表。

2. 在 **Health: All Clusters** 视图中，单击要查看 MetroCluster 复制详细信息的集群名称。在 **Cluster / Health details** 页面上，单击 **MetroCluster Replication** 选项卡。

   要复制的 MetroCluster 配置的拓扑显示在本地站点的相应集群对象区域中，其中包含有关正在镜像数据的远

程站点的信息。如果将指针移到图标上，则可以查看有关生成的事件的详细信息。

您可以使用“群集/运行状况详细信息”页面中显示的信息来纠正任何复制问题。如果在 MetroCluster 配置中发现镜像问题，则必须登录到 System Manager 或访问 ONTAP CLI 以解决问题。

相关信息

"集群/运行状况详细信息页面"

管理配额

了解 **Active IQ Unified Manager** 中的配额限制

用户配额限制是 Unified Manager 服务器用于评估用户的空间消耗是否接近限制或已达到用户配额设置的限制的值。如果超过软限制或达到硬限制，Unified Manager 服务器将生成用户配额事件。

默认情况下，Unified Manager 服务器将向已超过配额软限制或已达到配额硬限制并配置了用户配额事件的用户发送通知电子邮件。具有应用程序管理员角色的用户可以配置警报，将用户或用户组配额事件通知指定的收件人。

您可以使用 ONTAP System Manager 或 ONTAP CLI 指定配额限制。

在 **Active IQ Unified Manager** 中查看用户和用户组配额

Storage VM / 运行状况详细信息页面显示有关在 SVM 上配置的用户和用户组配额的信息。您可以查看用户或用户组的名称、对磁盘和文件设置的限制、已用磁盘和文件空间以及用于通知的电子邮件地址。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 存储 > 存储 **VM**。
2. 在 **Health: All Storage VMs** 视图中，选择 Storage VM，然后单击 **User and Group Quotas** 选项卡。

相关信息

"添加用户"

创建规则以在 **Active IQ Unified Manager** 中生成电子邮件地址

您可以创建规则，以根据与集群、存储虚拟机（SVM）、卷、qtree、用户或用户组相关联的用户配额指定电子邮件地址。当发生配额违规时，会向指定的电子邮件地址发送通知。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

- 您必须已阅读“生成用户和组配额电子邮件地址规则”页面上的指南。

您必须定义配额电子邮件地址的规则，并按要执行的顺序输入它们。例如，如果要使用电子邮件地址 abc@xyz.com 接收有关 abc 配额违规的通知，并为所有其他组使用电子邮件地址 dl-$GROUP@$DOMAIN，则必须按以下顺序列出规则：

- if ($USER == 'abc') then abc@xyz.com
- if ($GROUP == *) then dl-$GROUP@$DOMAIN

如果未满足指定规则的任何条件，则使用默认规则：

if ($USER_OR_GROUP == *) then $USER_OR_GROUP@$DOMAIN

步骤

1. 在左侧导航窗格中，单击 常规 > 配额电子邮件规则。
2. 根据您的条件输入规则。
3. 单击*验证*以验证规则的语法。

   如果规则的语法不正确，则显示错误消息。您必须更正语法并再次单击*验证*。

4. 单击 **Save**。
5. 确认您创建的电子邮件地址显示在 Storage **VM / Health** 详细信息页面的 **User and Group Quotas**（用户和组配额）选项卡中。

在 **Active IQ Unified Manager** 中为用户和用户组配额创建电子邮件通知格式

当存在配额相关问题（违反软限制或达到硬限制）时，您可以为发送给用户或用户组的电子邮件创建通知格式。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 常规 > 配额电子邮件格式。
2. 在*发件人*、*主题*和*电子邮件详细信息*字段中输入或修改详细信息。
3. 单击 **Preview** 以预览电子邮件通知。
4. 单击*关闭*以关闭预览窗口。
5. 如果需要，请修改电子邮件通知的内容。
6. 单击 **Save**。

在 **Active IQ Unified Manager** 中编辑用户和组配额电子邮件地址

您可以根据与集群、存储虚拟机（SVM）、卷、qtree、用户或用户组关联的用户配额修改电子邮件地址。当您想要覆盖在“生成用户和组配额电子邮件地址的规则”对话框中指定的规则所生成的电子邮件地址时，可以修改电子邮件地址。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 您必须已阅读 "创建规则的准则"。

如果编辑电子邮件地址，则生成用户和组配额电子邮件地址的规则不再适用于配额。要将通知发送到由指定规则生成的电子邮件地址，必须删除该电子邮件地址并保存更改。

步骤

1. 在左侧导航窗格中，单击*存储* > **SVMs**。
2. 在 **Health: All Storage VMs** 视图中，选择一个 SVM，然后单击 **User and Group Quotas** 选项卡。
3. 单击选项卡行下方的*编辑电子邮件地址*。
4. 在*编辑电子邮件地址*对话框中，执行相应的操作：

条件	操作
您希望将通知发送到指定规则生成的电子邮件地址	a. 删除*电子邮件地址*字段中的电子邮件地址。 b. 单击 **Save**。 c. 按 F5 刷新浏览器以重新加载“编辑电子邮件地址”对话框。由指定规则生成的电子邮件地址显示在电子邮件地址 字段中。
您希望将通知发送到指定的电子邮件地址	a. 修改*电子邮件地址*字段中的电子邮件地址。 b. 点击*保存*。生成用户和组配额电子邮件地址的规则不再适用于配额。

详细了解配额

了解 **Active IQ Unified Manager** 配额流程

配额可以是软配额或硬配额。软配额会导致 ONTAP 在超过指定限制时发送通知，而硬配额会在超过指定限制时阻止写入操作成功。

当 ONTAP 收到用户或用户组对某个 FlexVol 卷的写入请求时，它会检查是否已在该卷上激活该用户或用户组的配额，并确定以下内容：

- 是否达到硬限制

  如果是，则当达到硬限制并且发送硬配额通知时，写入操作将失败。

- 是否会突破软限制

  如果是，则当超出软限制并发送软配额通知时，写入操作将成功。

- 写入操作是否不会超过软限制

  如果是，则写入操作将成功，并且不会发送通知。

了解 **Active IQ Unified Manager** 中的配额

配额提供了一种限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数的方法。您可以使用 `/etc/quotas` 文件指定配额。配额应用于特定卷或 qtree。

了解 **Active IQ Unified Manager** 中的配额

您可以使用配额来限制 FlexVol 卷中的资源使用率，在资源使用率达到特定级别时提供通知，或跟踪资源使用率。

您指定配额的原因如下：

- 限制用户或组可使用的磁盘空间量或文件数量，或者限制一个 qtree 可包含的磁盘空间量或文件数量
- 在不施加限制的情况下跟踪用户、组或 qtree 使用的磁盘空间量或文件数量
- 在用户的磁盘或文件使用率较高时向用户发出警告

配额对话框的说明

使用 **Active IQ Unified Manager** 中的配额对话框

您可以使用运行状况：所有 Storage VM 视图中的用户和组配额选项卡中的相应选项来配置发生配额相关问题时发送的电子邮件通知的格式，并配置规则以根据用户配额指定电子邮件地址。

了解 **Active IQ Unified Manager** 中的电子邮件通知格式页面

电子邮件通知格式页面显示当存在配额相关问题（超出软限制或达到硬限制）时发送给用户或用户组的电子邮件的规则。

仅当生成以下用户或用户组配额事件时，才会发送电子邮件通知：已超出用户或组配额磁盘空间软限制、已超出用户或组配额文件数软限制、已达到用户或组配额磁盘空间硬限制，或已达到用户或组配额文件数硬限制。

- 发件人

  显示发送电子邮件的电子邮件地址，您可以对其进行修改。默认情况下，这是在“通知”页面上指定的电子邮件地址。

- 主题

  显示通知电子邮件的主题。

- 电子邮件详细信息

  显示通知电子邮件的文本。您可以根据需要修改文本。例如，您可以提供与配额属性相关的信息，并减少关键字数量。但是，您不应修改关键字。

  有效的关键字如下：

  - $EVENT_NAME

指定导致电子邮件通知的事件名称。

- $QUOTA_TARGET

  指定适用此配额的 qtree 或卷。

- $QUOTA_USED_PERCENT

  指定用户或用户组使用的磁盘硬限制、磁盘软限制、文件硬限制或文件软限制的百分比。

- $QUOTA_LIMIT

  指定用户或用户组达到的磁盘硬限制或文件硬限制，并生成以下事件之一：

  - 已达到用户或组配额磁盘空间硬限制
  - 已达到用户或组配额磁盘空间软限制
  - 已达到用户或组配额文件数硬限制
  - 已达到用户或组配额文件数软限制

- $QUOTA_USED

  指定用户或用户组使用的磁盘空间或创建的文件数。

- $QUOTA_USER

  指定用户或用户组名称。

命令按钮

命令按钮可用于预览、保存或取消对电子邮件通知格式所做的更改：

- 预览

  显示通知电子邮件的预览。

- 还原为出厂默认值

  使您能够将通知格式还原为出厂默认值。

- 保存

  保存对通知格式所做的更改。

了解 **Active IQ Unified Manager** 中的配额电子邮件地址规则

“生成用户和组配额电子邮件地址的规则”页面允许您创建规则，以根据与集群、SVM、卷、qtree、用户或用户组关联的用户配额指定电子邮件地址。当超出配额时，系统将向指定的电子邮件地址发送通知。

规则区域

您必须定义配额电子邮件地址的规则。您也可以添加注释来解释这些规则。

如何定义规则

必须按照要执行的顺序输入规则。如果满足第一个规则的条件，则根据此规则生成电子邮件地址。如果不满足条件，则考虑下一个规则的条件，依此类推。每行列出一个单独的规则。默认规则为列表中的最后一个规则。您可以更改规则的优先级顺序。但是，您无法更改默认规则的顺序。

例如，如果要使用电子邮件地址 qtree1@xyz.com 接收有关 qtree1 配额违规的通知，并对所有其他 qtree 使用电子邮件地址 admin@xyz.com，则规则必须按以下顺序列出：

- if ($QTREE == 'qtree1') then qtree1@xyz.com
- if ($QTREE == *) then admin@xyz.com

如果未满足指定规则的任何条件，则使用默认规则：

if ($USER_OR_GROUP == *) then $USER_OR_GROUP@$DOMAIN

如果多个用户具有相同的配额，则用户的名称将以逗号分隔的值显示，并且规则不适用于配额。

如何添加评论

您可以添加注释以解释规则。您应该在每个注释的开头使用 #，每行列出一个单独的注释。

规则语法

规则的语法必须是以下内容之一：

- if (`valid variableoperator *`) then `email ID@domain name`

  if 是关键字，且为小写。运算符为 ==。电子邮件 ID 可以包含任何字符、有效变量 $USER_OR_GROUP、$USER 或 $GROUP，或者任何字符与有效变量 $USER_OR_GROUP、$USER 或 $GROUP 的组合。域名可以包含任何字符、有效变量 $DOMAIN，或者任何字符与有效变量 $DOMAIN 的组合。有效变量可以是大写或小写，但不能是两者的组合。例如，$domain 和 $DOMAIN 是有效的，但 $Domain 不是有效变量。

- if (`valid variableoperator` `` `string` ``) then `email ID@domain name`

  if 是关键字且为小写。运算符可以是 contains 或 ==。电子邮件 ID 可以包含任何字符、有效变量 $USER_OR_GROUP、$USER 或 $GROUP，或者任何字符与有效变量 $USER_OR_GROUP、$USER 或 $GROUP 的组合。域名可以包含任何字符、有效变量 $DOMAIN，或者任何字符与有效变量 $DOMAIN 的组合。有效变量可以是大写或小写，但不能是两者的组合。例如，$domain 和 $DOMAIN 是有效的，但 $Domain 不是有效的变量。

命令按钮

使用命令按钮可以保存、验证或取消创建的规则：

- 验证

  验证创建的规则的语法。如果在验证过程中出现错误，则会显示生成错误的规则以及错误消息。

- 还原为出厂默认值

  使您能够将地址规则还原为出厂默认值。

- 保存

  验证规则的语法，如果没有错误，则保存规则。如果在验证过程中出现错误，则会显示生成错误的规则以及错误消息。

故障排除

向 **Unified Manager** 数据库目录添加磁盘空间

在 **Active IQ Unified Manager** 中向数据库目录添加磁盘空间

Unified Manager 数据库目录包含从 ONTAP 系统收集的所有运行状况和性能数据。在某些情况下，可能需要增加数据库目录的大小。

例如，如果 Unified Manager 从每个群集都有多个节点的大量群集收集数据，则数据库目录可能会变满。当数据库目录已满 90% 时，您将收到警告事件，当目录已满 95% 时，您将收到严重事件。

目录满 95% 后，不会再从集群中收集其他数据。

向数据目录添加容量所需的步骤不同，具体取决于 Unified Manager 是在 VMware ESXi 服务器上运行、在 Red Hat Linux 服务器上运行还是在 Microsoft Windows 服务器上运行。

在 **Active IQ Unified Manager** 中为 **VMware** 虚拟机的数据磁盘添加空间

如果需要增加 Unified Manager 数据库的数据磁盘上的空间量，可以在安装后通过使用 Unified Manager 维护控制台增加磁盘空间来添加容量。

开始之前

- 您必须能够访问 vSphere 客户端。
- 虚拟机必须没有本地存储的快照。
- 您必须具有维护用户凭据。

建议您在增加虚拟磁盘大小之前备份虚拟机。

步骤

1. 在 vSphere 客户端中，选择 Unified Manager 虚拟机，然后向数据 `disk 3`添加更多磁盘容量。有关详细信息，请参阅 VMware 文档。

   在某些罕见情况下，Unified Manager 部署使用“硬盘 2”而不是“硬盘 3”作为数据磁盘。如果在您的部署中发生此情况，请增加较大磁盘的空间。数据磁盘的空间将始终大于其他磁盘。

2. 在 vSphere 客户端中，选择 Unified Manager 虚拟机，然后选择*控制台*选项卡。
3. 在控制台窗口中单击，然后使用您的用户名和密码登录到维护控制台。

4. 在*主菜单*中，输入*系统配置*选项的数字。
5. 在*系统配置菜单*中，输入*增加数据磁盘大小*选项的数字。

在 **Active IQ Unified Manager** 中向 **Linux** 主机的数据目录添加空间

如果您在最初设置 Linux 主机并安装 Unified Manager 时为 `/opt/netapp/data`目录分配的磁盘空间不足以支持 Unified Manager，则可以在安装后通过增加 `/opt/netapp/data`目录上的磁盘空间来添加磁盘空间。

开始之前

您必须具有对安装了 Unified Manager 的 Red Hat Enterprise Linux 计算机的 root 用户访问权限。

建议您在增加数据目录大小之前备份 Unified Manager 数据库。

步骤

1. 以 root 用户身份登录到要添加磁盘空间的 Linux 计算机。
2. 按所示顺序停止 Unified Manager 服务和关联的 MySQL 软件： `systemctl stop ocieau ocie mysqld`
3. 创建具有足够磁盘空间的临时备份文件夹（例如 `/backup-data`），以包含当前 `/opt/netapp/data` 目录中的数据。
4. 将现有 `/opt/netapp/data`目录的内容和权限配置复制到备份数据目录：

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

5. 如果启用了 SE Linux：

   a. 获取现有 `/opt/netapp/data`文件夹中文件夹的 SE Linux 类型：

      ```
      se_type=`ls -Z /opt/netapp/data| awk '{print $4}'| awk -F: '{print $3}'| head -1
      ```

      系统将返回类似于以下内容的确认消息：

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. 运行 `chcon`命令以设置备份目录的 SE Linux 类型：

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. 删除 `/opt/netapp/data`目录的内容：

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. 通过 LVM 命令或添加额外磁盘，将 `/opt/netapp/data`目录的大小扩展到至少 150 GB。

如果您从磁盘创建了 /opt/netapp/data，则不应尝试将 /opt/netapp/data`作为 NFS 或 CIFS 共享进行挂载。因为在这种情况下，如果您尝试扩展磁盘空间，某些 LVM 命令（如 `resize`和 `extend）可能无法按预期工作。

8. 确认 `/opt/netapp/data`目录所有者（mysql）和组（root）未更改：

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

   系统将返回类似于以下内容的确认消息：

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

9. 如果启用了 SE Linux，请确认 /opt/netapp/data 目录的上下文仍然设置为 mysqld_db_t：

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

      系统将返回类似于以下内容的确认消息：

   ```
   -rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
   /opt/netapp/data/abc
   ```

10. 删除该文件 abc，以便此无关文件将来不会导致数据库错误。
11. 将内容从 `backup-data`复制回扩展的 `/opt/netapp/data`目录：

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

12. 如果启用了 SE Linux，请运行以下命令：

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

13. 启动 MySQL 服务：

    ```
    systemctl start mysqld
    ```

14. MySQL 服务启动后，按所示顺序启动 ocie 和 ocieau 服务：

    ```
    systemctl start ocie ocieau
    ```

15. 所有服务启动后，删除备份文件夹 /backup-data：

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

在 **Active IQ Unified Manager** 中为 **Microsoft Windows** 服务器的逻辑驱动器添加空间

如果需要增加 Unified Manager 数据库的磁盘空间量，可以向安装 Unified Manager 的逻

辑驱动器添加容量。

开始之前

您必须具有 Windows 管理员权限。

我们建议您在添加磁盘空间之前备份 Unified Manager 数据库。

步骤

1. 以管理员身份登录到要添加磁盘空间的 Windows 服务器。
2. 请按照要添加更多空间的方法对应的步骤操作：

选项	问题描述
在物理服务器上，向安装有 Unified Manager 服务器的逻辑驱动器添加容量。	按照 Microsoft 主题中的步骤操作： "扩展基本卷"
在物理服务器上，添加硬盘驱动器。	按照 Microsoft 主题中的步骤操作： "添加硬盘驱动器"
在虚拟机上，增加磁盘分区的大小。	按照 VMware 主题中的步骤操作： "增加磁盘分区的大小"

在 **Active IQ Unified Manager** 中更改性能统计信息收集间隔

性能统计的默认收集间隔为 5 分钟。如果发现大型集群的收集未在默认时间内完成，则可以将此时间间隔更改为 10 或 15 分钟。此设置会影响此 Unified Manager 实例正在监控的所有集群的统计信息收集。

开始之前

您必须拥有已授权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。

性能统计数据收集未按时完成的问题由横幅消息指示 `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>.`

只有在因统计信息收集问题而需要时，才应更改收集间隔。请勿出于任何其他原因更改此设置。

> 将此值从默认设置 5 分钟更改后，可能会影响 Unified Manager 报告的性能事件的数量和频率。例如，当超出策略 30 分钟时，系统定义的性能阈值会触发事件。使用 5 分钟收集时，必须连续六次收集超出策略。对于 15 分钟的收集，只需在两个收集期内超出策略即可。

集群设置页面底部的消息指示当前统计数据收集间隔。

步骤

1. 使用 SSH 作为维护用户登录到 Unified Manager 主机。

   此时将显示 Unified Managermaintenance 控制台提示。

2. 键入标记为*性能轮询间隔配置*的菜单选项的编号，然后按 Enter。
3. 如果出现提示，请再次输入维护用户密码。
4. 键入要设置的新轮询间隔的数值，然后按 Enter 键。

如果您将 Unified Manager 收集时间间隔更改为 10 或 15 分钟，并且当前连接到外部数据提供程序（如 Graphite），则必须更改数据提供程序传输时间间隔，使其等于或大于 Unified Manager 收集时间间隔。

更改 **Active IQ Unified Manager** 保留事件和性能数据的时间长度

默认情况下，Unified Manager 将所有受监控集群的事件数据和性能数据存储 6 个月。此后，系统会自动删除旧数据，以便为新数据腾出空间。此默认时间范围适用于大多数配置，但包含许多集群和节点的大型配置可能需要缩短保留期，以便 Unified Manager 以最佳方式运行。

开始之前

您必须具有应用程序管理员角色。

您可以在“数据保留”页面中更改这两种类型数据的保留期。这些设置会影响此 Unified Manager 实例正在监控的所有集群的数据保留。

Unified Manager 每 5 分钟收集一次性能统计信息。每天将 5 分钟统计数据汇总为每小时性能统计数据。它保留 30 天的 5 分钟历史性能数据和 6 个月的每小时汇总性能数据（默认情况下）。

只有在空间不足或备份和其他操作需要很长时间才能完成时，才应缩短保留期。缩短保留期具有以下效果：

- 午夜后，旧的性能数据将从 Unified Manager 数据库中删除。
- 旧事件数据将立即从 Unified Manager 数据库中删除。
- 保留期之前的事件将无法再在用户界面中查看。
- 在保留期之前，UI 中显示每小时性能统计信息的位置将为空白。
- 如果事件保留期超过性能数据保留期，性能滑块下将显示一条消息，警告旧的性能事件可能在其关联的图表中没有支持数据。

步骤

1. 在左侧导航窗格中，单击*策略* > 数据保留。
2. 在*数据保留*页面中，选择事件保留或性能数据保留区域中的滑块工具，并将其移动到应保留数据的月数，然后单击*保存*。

解决 **Active IQ Unified Manager** 中的未知身份验证错误

执行与身份验证相关的操作（如添加、编辑、删除或测试远程用户或组）时，可能会显示以下错误消息： `Unknown authentication error.`

原因

如果您为下列选项设置了不正确的值，则可能会出现此问题：

- Active Directory 身份验证服务的管理员名称
- OpenLDAP 身份验证服务的绑定可分辨名称

更正操作

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 根据选定的身份验证服务，输入管理员名称或绑定可分辨名称的相应信息。
3. 单击*测试身份验证*，使用您指定的详细信息测试身份验证。
4. 单击 **Save**。

解决 **Active IQ Unified Manager** 中的"用户未找到"错误

执行与身份验证相关的操作（如添加、编辑、删除或测试远程用户或组）时，将显示以下错误消息： `User not found.`

原因

如果用户存在于 AD 服务器或 LDAP 服务器中，并且您将基本可分辨名称设置为了不正确的值，则可能会出现此问题。

更正操作

1. 在左侧导航窗格中，单击*常规* > 远程身份验证。
2. 输入基本可分辨名称的相应信息。
3. 单击 **Save**。

解决在 **Active IQ Unified Manager** 中使用其他身份验证服务添加 **LDAP** 时引起的问题

当您选择“其他”作为身份验证服务时，用户和组“对象类”将保留先前选定模板中的值。如果 LDAP 服务器不使用相同的值，则操作可能会失败。

原因

用户在 OpenLDAP 中配置有误。

更正操作

可以使用以下解决方法之一手动解决此问题。

如果您的 LDAP 用户对象类和组对象类分别是 user 和 group，请执行以下步骤：

1. 在左侧导航窗格中，单击常规 > 远程身份验证。
2. 在*身份验证服务*下拉菜单中，选择 **Active Directory**，然后选择*其他*。
3. 填写文本字段。

如果您的 LDAP 用户对象类和组对象类分别为 posixAccount 和 posixGroup，请执行以下步骤：

1. 在左侧导航窗格中，单击 常规 > 远程身份验证。
2. 在*身份验证服务*下拉菜单中，选择*OpenLDAP*，然后选择*其他*。
3. 填写文本字段。

如果前两个解决方法不适用，请调用 `option-set` API，并将 `auth.ldap.userObjectClass`和 `auth.ldap.groupObjectClass`选项设置为正确的值。

解决 **Active IQ Unified Manager** 中的 **NetApp Manageability SDK** 日志轮换问题

将基于 ONTAPI API 的集群添加到 Windows 操作系统上的 Unified Manager 后，`nmsdk.log` 文件大小会增加并超过 10 MB 的大小限制。

原因

如果未发生日志轮换，则可能会发生此问题。

更正操作

1. 停止 Unified Manager。
2. 在 Windows 上安装 Unified Manager 时，请安装 Logrotate 版本 0.0.0.18。有关详细信息，请参见"NetApp Manageability SDK 技术报告的安全强化指南"。
3. 启动 Unified Manager。

管理事件和警报

管理事件

了解 **Active IQ Unified Manager** 中的 **Active IQ** 平台事件

Unified Manager 可显示 Active IQ 平台发现的事件。这些事件是通过针对由 Unified Manager 监视的所有存储系统生成的 AutoSupport 消息运行一组规则来创建的。

有关详细信息，请参见"如何生成 Active IQ 平台事件"。

Unified Manager 会自动检查新规则文件，并且仅在有新规则时才下载新文件。在没有外部网络访问权限的站点中，您需要从*存储管理* > 事件设置 > *上传规则*手动上传规则。

这些 Active IQ 事件不会与现有的 Unified Manager 事件重叠，它们可识别与系统配置、布线、最佳实践和可用性问题相关的突发事件或风险。

有关启用平台事件的详细信息，请参见"启用 Active IQ 门户事件"。有关上传规则文件的详细信息，请参见"上传新 Active IQ 规则文件"。

NetApp Active IQ 是一种基于云的服务，可提供预测分析和主动支持，以优化整个 NetApp 混合云的存储系统运行。有关详细信息，请参见 "NetApp Active IQ"。

Event Management System 事件是什么

了解 **Active IQ Unified Manager** 中的事件管理系统事件

Event Management System (EMS) 从 ONTAP 内核的不同部分收集事件数据，并提供事件转发机制。这些 ONTAP 事件可以在 Unified Manager 中报告为 EMS 事件。集中式监控和管理简化了基于这些 EMS 事件的关键 EMS 事件和警报通知的配置。

将集群添加到 Unified Manager 时，会将 Unified Manager 地址作为通知目标添加到集群。EMS 事件在集群中发生后立即报告。

在 Unified Manager 中接收 EMS 事件有两种方法：

- 一定数量的重要 EMS 事件会自动报告。
- 您可以订阅接收单个 EMS 事件。

Unified Manager 生成的 EMS 事件会根据生成事件的方法进行不同的报告：

功能	自动 **EMS** 消息	订阅的 **EMS** 消息
可用的 EMS 事件	EMS 事件的子集	所有 EMS 事件
触发时的 EMS 消息名称	Unified Manager 事件名称（从 EMS 事件名称转换而来）	非特定，格式为“Error EMS received”。详细消息提供实际 EMS 事件的点符号格式

功能	自动 **EMS** 消息	订阅的 **EMS** 消息
收到的消息	一旦发现此集群	在将每个所需的 EMS 事件添加到 Unified Manager 之后，以及在接下来的 15 分钟轮询周期之后
事件生命周期	与其他 Unified Manager 事件相同：新建、已确认、已解决和已废弃状态	在事件创建 15 分钟后，集群刷新后，EMS 事件将被废弃
在 Unified Manager 停机期间捕获事件	是，当系统启动时，它与每个集群通信以获取缺失的事件	否
事件详情	建议的纠正措施直接从 ONTAP 导入，以提供一致的解决方案	事件详细信息页面中无可用的纠正措施

一些新的自动 EMS 事件是指示先前事件已解决的信息事件。例如，“FlexGroup Constituents Space Status All OK”信息事件指示“FlexGroup Constituents Have Space Issues”错误事件已解决。信息事件不能使用与其他事件严重性类型相同的事件生命周期来管理，但是，如果同一卷收到另一个“`Space Issues`”错误事件，则该事件将自动废弃。

自动添加到 **Active IQ Unified Manager** 的 **EMS** 事件

以下 ONTAP EMS 事件将自动添加到 Unified Manager。这些事件将在 Unified Manager 正在监视的任何群集上触发时生成。

当监控运行 ONTAP 9.5 或更高版本软件的集群时，可使用以下 EMS 事件：

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重程度
用于聚合重新定位的云层访问被拒绝	arl.netra.ca.check.failed	聚合	错误
存储故障转移期间用于聚合重新定位的云层访问被拒绝	gb.netra.ca.check.failed	聚合	错误
FabricPool 镜像复制重新同步已完成	wafl.ca.resync.complete	集群	错误
FabricPool 空间接近全满	fabricpool.nearly.full	集群	错误
NVMe-oF 宽限期已开始	nvmf.graceperiod.start	集群	警告
NVMe-oF 宽限期处于活动状态	nvmf.graceperiod.active	集群	警告
NVMe-oF 宽限期已结束	nvmf.graceperiod.expired	集群	警告
LUN 已销毁	lun.destroy	LUN	信息
Cloud AWS MetaDataConnFail	cloud.aws.metadataConnFail	节点	错误
Cloud AWS IAMCredsExpired	cloud.aws.iamCredsExpired	节点	错误

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重程度
Cloud AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	节点	错误
Cloud AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	节点	错误
Cloud AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	节点	信息
Cloud AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	节点	错误
Cloud AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	节点	错误
无法解析云层主机	objstore.host.unresolvable	节点	错误
云层集群间网络接口已关闭	objstore.interclusterlifDown	节点	错误
请求与云层签名不匹配	osc.signatureMismatch	节点	错误
一个 NFSv4 池已用尽	Nblade.nfsV4PoolExhaust	节点	关键
QoS 监控内存已达到上限	qos.monitor.memory.maxed	节点	错误
QoS 监控内存已缩减	qos.monitor.memory.abated	节点	信息
NVMeNS 已销毁	NVMeNS.destroy	命名空间	信息
NVMeNS 联机	NVMeNS.offline	命名空间	信息
NVMeNS 脱机	NVMeNS.online	命名空间	信息
NVMeNS 空间不足	NVMeNS.out.of.space	命名空间	警告
同步复制未同步	sms.status.out.of.sync	SnapMirror 关系	警告
同步复制已还原	sms.status.in.sync	SnapMirror 关系	信息
同步复制自动重新同步失败	sms.resync.attempt.failed	SnapMirror 关系	错误
多个 CIFS 连接	Nblade.cifsManyAuths	SVM	错误
超出 CIFS 连接数上限	Nblade.cifsMaxOpenSameFile	SVM	错误
超出每用户 CIFS 连接数上限	Nblade.cifsMaxSessPerUsrConn	SVM	错误
CIFS NetBIOS 名称冲突	Nblade.cifsNbNameConflict	SVM	错误
尝试连接不存在的 CIFS 共享	Nblade.cifsNoPrivShare	SVM	关键
CIFS 卷影复制操作失败	cifs.shadowcopy.failure	SVM	错误
AV 服务器发现病毒	Nblade.vscanVirusDetected	SVM	错误

Unified Manager 事件名称	**EMS** 事件名称	受影响的资源	**Unified Manager** 严重程度
没有可用于病毒扫描的 AV 服务器连接	Nblade.vscanNoScannerConn	SVM	关键
未注册 AV 服务器	Nblade.vscanNoRegdScanner	SVM	错误
AV 服务器连接无响应	Nblade.vscanConnInactive	SVM	信息
AV 服务器太忙，无法接受新的扫描请求	Nblade.vscanConnBackPressure	SVM	错误
用户未经授权尝试访问 AV 服务器	Nblade.vscanBadUserPrivAccess	SVM	错误
FlexGroup 成分卷存在空间问题	flexgroup.constituents.have.space.issues	卷	错误
FlexGroup 成分卷空间状态一切正常	flexgroup.constituents.space.status.all.ok	卷	信息
FlexGroup 成分卷存在索引节点问题	flexgroup.constituents.have.inodes.issues	卷	错误
FlexGroup 成分卷索引节点状态一切正常	flexgroup.constituents.inodes.status.all.ok	卷	信息
卷逻辑空间接近全满	monitor.vol.nearFull.inc.sav	卷	警告
卷逻辑空间全满	monitor.vol.full.inc.sav	卷	错误
卷逻辑空间正常	monitor.vol.one.ok.inc.sav	卷	信息
WAFL 卷 AutoSize 失败	wafl.vol.autoSize.fail	卷	错误
WAFL 卷自动调整大小已完成	wafl.vol.autoSize.done	卷	信息
WAFL READDIR 文件操作超时	wafl.readdir.expired	卷	错误

在 **Active IQ Unified Manager** 中订阅 **ONTAP EMS** 事件

您可以订阅接收由安装了 ONTAP 软件的系统生成的事件管理系统（EMS）事件。EMS 事件的一个子集会自动报告给 Unified Manager，但只有在您订阅了这些事件时，才会报告其他 EMS 事件。

开始之前

不要订阅已自动添加到 Unified Manager 的 EMS 事件，因为在接收同一问题的两个事件时，这可能会导致混淆。

您可以订阅任意数量的 EMS 事件。系统将验证您订阅的所有事件，并且仅将已验证的事件应用于您在 Unified Manager 中监控的集群。*ONTAP 9 EMS* 事件目录 提供指定版本的 ONTAP 9 软件的所有 EMS 消息的详细信息。从 ONTAP 9 产品文档页面中找到相应版本的 *EMS* 事件目录，以获取适用事件的列表。

"ONTAP 9 产品库"

您既可以为订阅的 ONTAP EMS 事件配置警报，也可以为这些事件创建要执行的自定义脚本。

如果未收到已订阅的 ONTAP EMS 事件，则集群的 DNS 配置可能存在问题，导致集群无法访问 Unified Manager 服务器。要解决此问题，集群管理员必须更正集群的 DNS 配置，然后重新启动 Unified Manager。这样做会将挂起的 EMS 事件刷新到 Unified Manager 服务器。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 事件设置。
2. 在事件设置页面中，单击*订阅 EMS 事件*按钮。
3. 在订阅 EMS 事件对话框中，输入要订阅的 ONTAP EMS 事件的名称。

   要从 ONTAP 集群 shell 查看您可以订阅的 EMS 事件的名称，您可以使用 `event route show` 命令（在 ONTAP 9 之前）或 `event catalog show` 命令（ONTAP 9 或更高版本）。

   "如何在 Active IQ Unified Manager 中配置并接收来自 ONTAP EMS 事件订阅的警报"

4. 单击 **Add**。

   EMS 事件已添加至已订阅 EMS 事件列表，但“适用于群集”列显示您添加的 EMS 事件的状态为“Unknown”。

5. 单击*保存并关闭*以在集群中注册 EMS 事件订阅。
6. 再次点击 订阅 **EMS** 事件。

   状态 “是” 出现在您添加的 EMS 事件的“适用于集群”列中。

   如果状态不是 “Yes”，请检查 ONTAP EMS 事件名称的拼写。如果输入的名称不正确，则必须删除不正确的事件，然后再次添加该事件。

当 ONTAP EMS 事件发生时，该事件将显示在“事件”页面上。您可以在“事件详细信息”页面中选择该事件，以查看有关 EMS 事件的详细信息。您还可以管理事件的处置或为该事件创建警报。

了解 **Active IQ Unified Manager** 如何处理收到的事件

当 Unified Manager 收到事件时，它将显示在“仪表板”页面、“事件管理”清单页面、“集群/性能”页面的“摘要”和“资源管理器”选项卡以及特定对象的清单页面（例如，“卷/运行状况”清单页面）中。

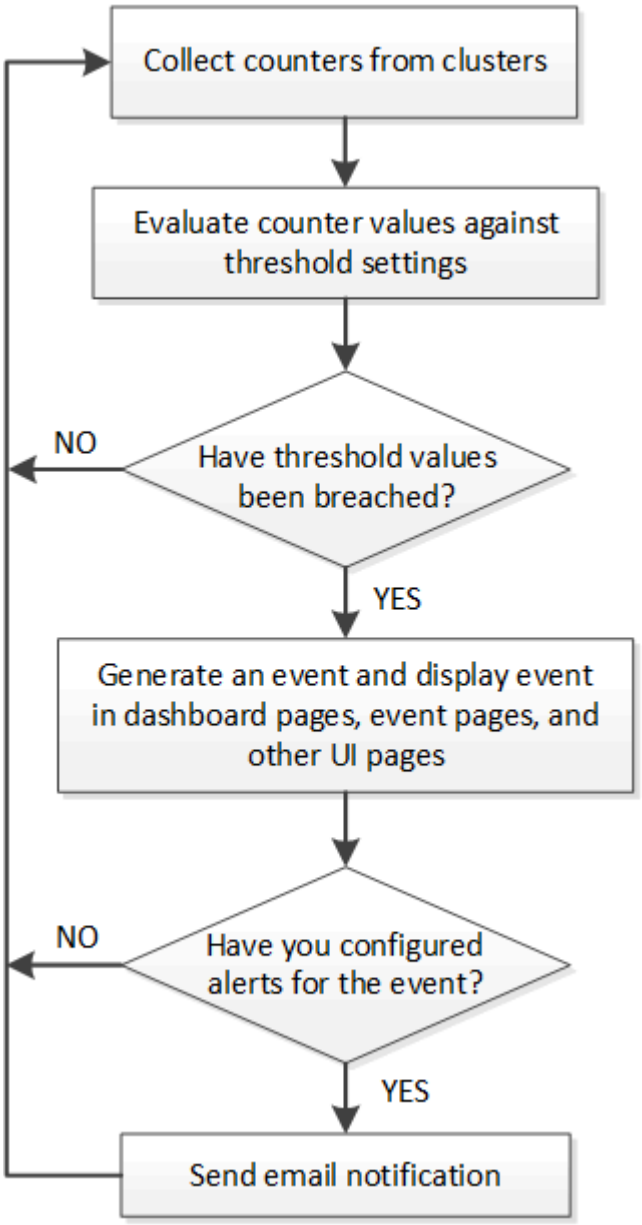
当 Unified Manager 检测到同一集群组件连续多次出现相同的事件条件时，它会将所有这些情况视为单个事件，而不是单独的事件。事件的持续时间会递增，以指示该事件仍处于活动状态。

根据您在“警报设置”页面中配置设置的方式，您可以将这些事件通知其他用户。警报会导致启动以下操作：

- 可以向所有 Unified Manager 管理员用户发送有关该事件的电子邮件。
- 该事件可以发送给其他电子邮件收件人。
- SNMP 陷阱可以发送到陷阱接收器。

- 可以执行自定义脚本来执行操作。

此工作流程如下图所示。



在 **Active IQ Unified Manager** 中查看事件详细信息

您可以查看由 Unified Manager 触发以采取纠正措施的事件的详细信息。例如，如果存在运行状况事件 Volume Offline，则可以单击该事件以查看详细信息并执行纠正措施。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

事件详细信息包括事件的来源、事件的原因以及与事件相关的任何注释等信息。

步骤

1. 在左侧导航窗格中，单击*事件管理*。

默认情况下，“所有活动事件”视图将显示过去 7 天内生成的具有事件或风险影响级别的新事件和已确认（活动）事件。

2. 如果要查看特定类别的事件（例如容量事件或性能事件），请单击 **View** ，然后从事件类型菜单中进行选择。
3. 单击要查看其详细信息的事件名称。

   事件详细信息显示在事件详细信息页面中。

在 **Active IQ Unified Manager** 中查看未分配的事件

您可以查看未分配的事件，然后将每个事件分配给可以解决它们的用户。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*事件管理*。

   默认情况下，“新建”和“已确认”事件将显示在“事件管理”清单页面上。

2. 在*过滤器*窗格中，在*分配给*区域中选择*未分配*过滤器选项。

确认并解决 **Active IQ Unified Manager** 中的事件

在开始处理触发事件的问题之前，您应先确认该事件，以避免持续收到重复的警报通知。针对特定事件采取纠正措施后，您应将该事件标记为已解决。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

您可以同时确认和解决多个事件。

您无法确认信息事件。

步骤

1. 在左侧导航窗格中，单击*事件管理*。
2. 从事件列表中，执行以下操作以确认这些事件：

目的	操作
确认单个事件并将其标记为已解决	a. 单击事件名称。 b. 从事件详细信息页面确定事件的原因。 c. 单击*确认*。 d. 采取适当的纠正措施。 e. 单击*标记为已解决*。

目的	操作
确认多个事件并将其标记为已解决	a. 从相应的事件详细信息页面确定事件的原因。 b. 选择事件。 c. 单击*确认*。 d. 采取适当的纠正措施。 e. 单击*标记为已解决*。

在事件被标记为已解决后，该事件将被移动到已解决的事件列表中。

3. 可选：在*备注和更新*区域中，添加有关您如何处理事件的备注，然后单击*发布*。

在 **Active IQ Unified Manager** 中将事件分配给特定用户

您可以将未分配的事件分配给自己或其他用户，包括远程用户。如果需要，您可以将已分配的事件重新分配给其他用户。例如，当存储对象上频繁出现问题时，您可以将这些问题的事件分配给管理该对象的用户。

开始之前

- 必须正确配置用户名和电子邮件 ID。
- 您必须具有操作员、应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*事件管理*。
2. 在*事件管理*库存页面中，选择要分配的一个或多个事件。
3. 通过选择以下选项之一来分配事件：

如果要将此事件分配给.....	操作
您自己	单击 分配给 > 我。
其他用户	a. 单击*分配给* > 其他用户。 b. 在“分配所有者”对话框中，输入用户名，或从下拉列表中选择用户。 c. 单击*分配*。 电子邮件通知将发送给用户。 如果不输入用户名或从下拉列表中选择用户，然后单击*分配*，则事件将保持未分配状态。

在 **Active IQ Unified Manager** 中禁用不需要的事件

默认情况下，所有事件均处于启用状态。您可以全局禁用事件，以防止为环境中不重要的

事件生成通知。您可以在要恢复接收通知时启用已禁用的事件。

开始之前

您必须具有应用程序管理员或存储管理员角色。

禁用事件时，系统中以前生成的事件将被标记为已废弃，并且不会触发为这些事件配置的警报。启用已禁用的事件后，将从下一监控周期开始生成这些事件的通知。

如果禁用某个对象的事件（例如， `vol offline` 事件），然后再启用该事件，则 Unified Manager 不会为在事件处于禁用状态时离线的对象生成新事件。Unified Manager 仅在重新启用事件后对象状态发生变化时才会生成新事件。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 事件设置。
2. 在*事件设置*页面中，通过选择以下选项之一来禁用或启用事件：

目的	操作
禁用事件	a. 单击 **Disable**。 b. 在禁用事件对话框中，选择事件严重性。 c. 在匹配事件列中，根据事件严重性选择要禁用的事件，然后单击右箭头将这些事件移动到禁用事件列。 d. 单击*保存并关闭*。 e. 验证已禁用的事件是否显示在“事件设置”页面的列表视图中。
启用事件	a. 选中要启用的一个或多个事件的复选框。 b. 单击 启用。

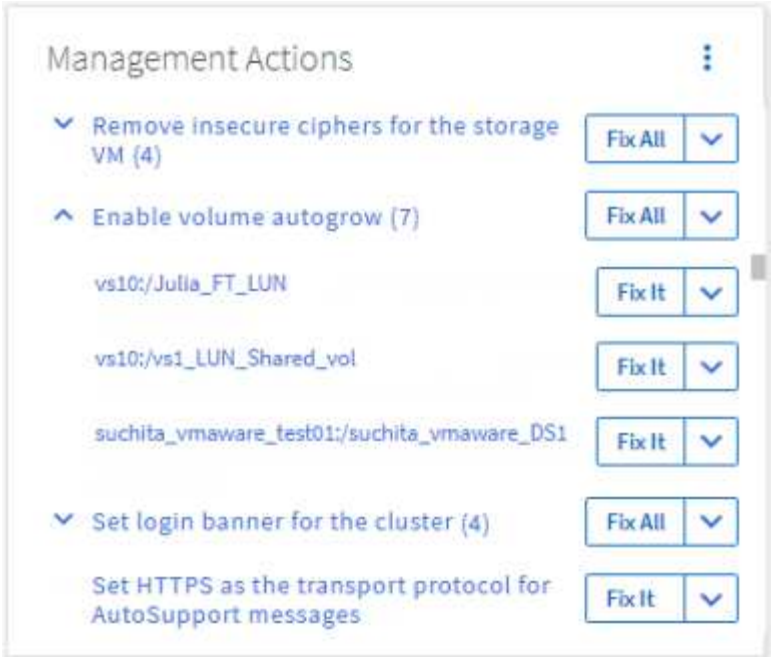
使用 **Active IQ Unified Manager** 中的自动修复功能修复问题

Unified Manager 可以使用 **Fix It** 按钮彻底诊断某些事件并提供单一解决方案。如果可用，这些解决方案将显示在仪表板、事件详细信息页面和左侧导航菜单上的工作负载分析选项中。

大多数事件都有各种可能的解决方案，这些解决方案显示在事件详细信息页面中，因此您可以使用 ONTAP System Manager 或 ONTAP CLI 实施最佳解决方案。当 Unified Manager 确定存在解决此问题的单一解决方案，并且可以使用 ONTAP CLI 命令解决此问题时，可以使用 **Fix It** 操作。

步骤

1. 要查看可通过*仪表板*修复的事件，请点击*仪表板*。



2. 要解决 Unified Manager 可以修复的任何问题，请单击 修复它 按钮。要修复多个对象上存在的问题，请单击 全部修复 按钮。

有关可通过自动修正修复的问题的信息，请参见 "Unified Manager 可以解决哪些问题"。

在 **Active IQ Unified Manager** 中启用和禁用 **Active IQ** 事件报告

默认情况下，Active IQ 平台事件将生成并显示在 Unified Manager 用户界面中。如果您发现这些事件过于“嘈杂”，或者您不希望在 Unified Manager 中查看这些事件，则可以禁止生成这些事件。如果您想恢复接收这些通知，可以稍后再启用它们。

开始之前

您必须具有应用程序管理员角色。

禁用此功能后，Unified Manager 将立即停止接收 Active IQ 平台事件。

启用此功能后，Unified Manager 会根据集群的时区在午夜后不久开始接收 Active IQ 平台事件。开始时间基于 Unified Manager 从每个集群接收 AutoSupport 消息的时间。

步骤

1. 在左侧导航窗格中，单击*常规* > 功能设置。
2. 在*功能设置*页面中，通过选择以下选项之一禁用或启用 Active IQ 平台事件：

目的	操作
禁用 Active IQ 平台事件	在 **Active IQ** 门户事件 面板中，向左移动滑块按钮。
启用 Active IQ 平台事件	在*Active IQ 门户事件*面板中，向右移动滑块按钮。

在 **Active IQ Unified Manager** 中上传新的 **Active IQ** 规则文件

Unified Manager 会自动检查新的 Active IQ 事件（规则）文件，并在有更新规则时下载新文件。但是，在没有外部网络访问权限的站点中，您需要手动上传规则文件。

Active IQ 规则也称为 Config Advisor （CA） 安全规则。

当您在没有网络连接的站点中将 Unified Manager 安装或升级到特定版本时，捆绑的 Active IQ 规则将自动可用于上传。但是，建议您大约每月从 NetApp 支持站点下载一次新的规则文件，以确保生成更新的事件，并且您的存储系统继续保持最佳性能。

开始之前

- 必须启用 Active IQ 门户事件报告。默认情况下，此功能处于启用状态。有关信息，请参见 "启用 Active IQ 门户事件"。
- 您必须从 NetApp 支持站点下载规则文件。

  规则文件位于： https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

步骤

1. 在具有网络访问权限的计算机上，导航到 NetApp 支持站点并下载当前规则 `.zip`文件。

   捆绑的规则包包括规则存储库、数据源和 NetApp 知识库文章。

   在 Windows 系统上，在没有网络连接的站点中，默认情况下，NetApp 知识库文章不会与安装程序捆绑在一起。您可以从支持站点下载 *secure_rules.zip* 文件并上传，以查看所有规则的知识库文章。

2. 将规则文件传输到您可以带入安全区域的某些介质，然后将其复制到安全区域的系统上。
3. 在左侧导航窗格中，单击*存储管理* > 事件设置。
4. 在 **Event Setup** 页面中，单击 **Upload Rules** 按钮。
5. 在*上传规则*对话框中，导航到并选择您下载的规则 `.zip`文件，然后单击*上传*。

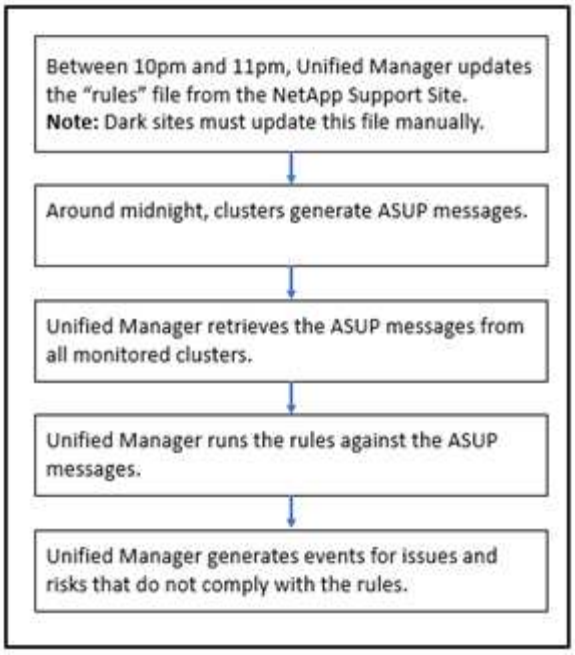
   此过程可能需要几分钟时间。

规则文件将在 Unified Manager 服务器上解压缩。在您的托管集群于午夜后生成 AutoSupport 文件后，Unified Manager 将根据规则文件检查集群，并根据需要生成新的风险和突发事件。

有关详细信息，请参见此知识库（KB）文章： "如何在 Active IQ Unified Manager 中手动更新 AIQCASecure 规则"。

Active IQ Unified Manager 如何生成 **Active IQ** 平台事件

Active IQ 平台事件和风险将转换为 Unified Manager 事件，如下图所示。

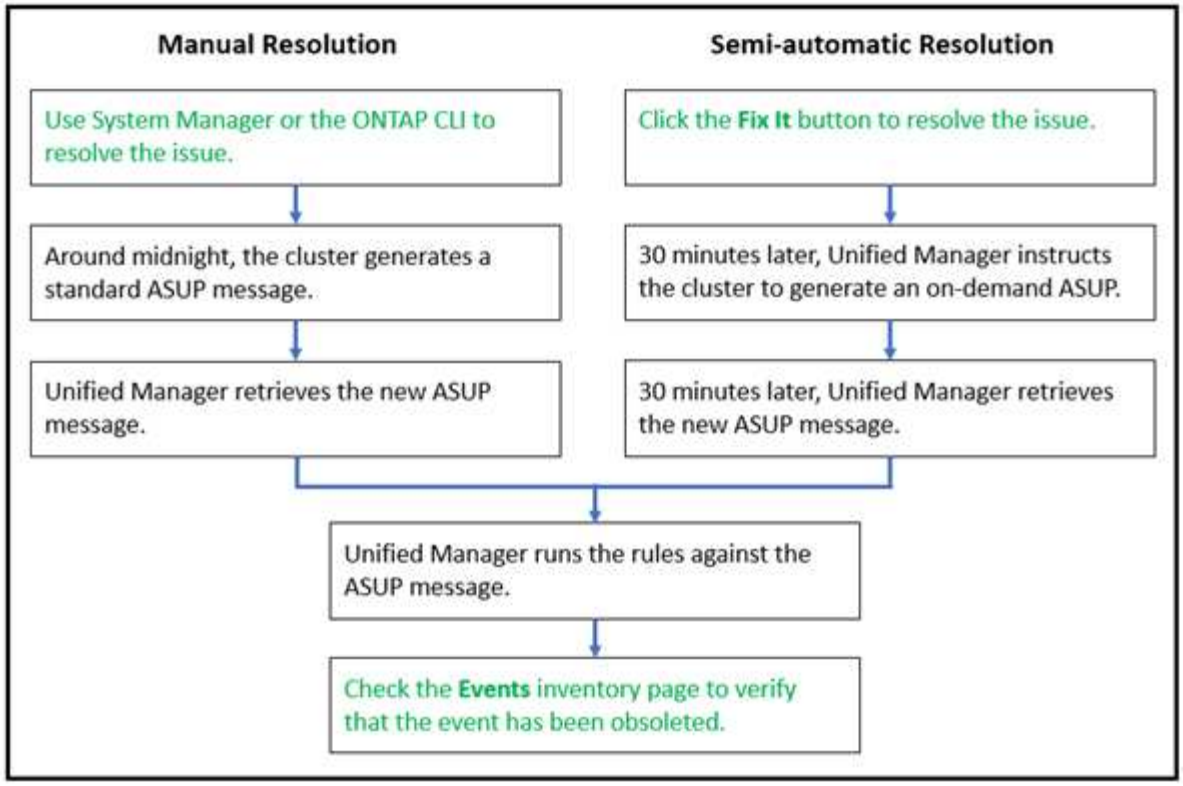


如您所见，Active IQ 平台上编译的规则文件保持最新，每天生成群集 AutoSupport 消息，Unified Manager 每天更新事件列表。

在 **Active IQ Unified Manager** 中解决 **Active IQ** 平台事件

Active IQ 平台事件和风险与其他 Unified Manager 事件类似，因为它们可以分配给其他用户进行解决，并且它们具有相同的可用状态。但是，当您使用 **Fix It** 按钮解决这些类型的事件时，您可以在数小时内验证解决方案。

下图显示了在解决从 Active IQ 平台生成的事件时，您必须采取的操作（绿色）以及 Unified Manager 采取的操作（黑色）。



执行手动解决时，您必须登录到 System Manager 或 ONTAP 命令行界面来修复此问题。只有在集群于午夜生成新的 AutoSupport 消息后，您才能验证此问题。

使用 **Fix It** 按钮执行半自动修复时，您可以在数小时内验证修复是否成功。

在 **Active IQ Unified Manager** 中配置事件保留设置

您可以指定事件在自动删除之前在 Unified Manager 服务器中保留的月数。

开始之前

您必须具有应用程序管理员角色。

将事件保留超过 6 个月可能会影响服务器性能，不建议这样做。

步骤

1. 在左侧导航窗格中，单击*常规* > 数据保留。
2. 在*数据保留*页面中，选择事件保留区域中的滑块，并将其移动到应保留事件的月数，然后单击*保存*。

什么是 **Unified Manager** 维护窗口

了解 **Active IQ Unified Manager** 维护窗口

您可以定义 Unified Manager 维护窗口，以便在已安排群集维护且不希望收到大量不需要的通知时，在特定时间范围内抑制事件和警报。

维护窗口启动时，“Object Maintenance Window Started”事件将发布到 Event Management 清单页面。此事件在维护窗口结束时会自动失效。

在维护窗口期间，仍会生成与该集群上所有对象相关的事件，但它们不会出现在任何 UI 页面中，并且不会为这些事件发送警报或其他类型的通知。但是，您可以通过选择“事件管理”清单页面上的“查看”选项之一，来查看在维护窗口期间为所有存储对象生成的事件。

您可以安排将来启动的维护窗口，可以更改计划维护窗口的开始和结束时间，也可以取消计划维护窗口。

安排维护时段以禁用 **Active IQ Unified Manager** 中的集群事件通知

如果您有计划的群集停机时间，例如升级群集或移动其中一个节点，则可以通过安排 Unified Manager 维护窗口来抑制通常在该时间范围内生成的事件和警报。

开始之前

您必须具有应用程序管理员或存储管理员角色。

在维护窗口期间，仍会生成与该集群上的所有对象相关的事件，但它们不会显示在事件页面中，并且不会为这些事件发送警报或其他类型的通知。

您为维护时段输入的时间基于 Unified Manager 服务器的时间。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 集群设置。
2. 在集群的*维护模式*列中，选择滑块按钮并将其向右移动。

   此时将显示日历窗口。

3. 选择维护窗口的开始和结束日期和时间，然后单击*应用*。

   “Scheduled” 消息出现在滑块按钮旁边。

到达开始时间时，集群进入维护模式，并生成“对象维护窗口已启动”事件。

更改或取消 **Active IQ Unified Manager** 中已计划的维护窗口

如果已将 Unified Manager 维护窗口配置为在将来发生，则可以更改开始和结束时间或取消维护窗口。

开始之前

您必须具有应用程序管理员或存储管理员角色。

如果在计划的维护窗口结束时间之前完成了集群维护，并且希望再次开始接收来自集群的事件和警报，则取消当前运行的维护窗口非常有用。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 集群设置。
2. 在集群的*维护模式*列中：

目的	执行此步骤……
更改计划维护窗口的时间范围	a. 单击滑块按钮旁边的文本“Scheduled”。 b. 更改开始和/或结束日期和时间，然后单击*应用*。
延长活动维护窗口的持续时间	a. 单击滑块按钮旁边的文本“活动”。 b. 更改结束日期和时间，然后单击*应用*。
取消计划的维护时间段	选择滑块按钮并将其向左移动。
取消活动的维护时段	选择滑块按钮并将其向左移动。

查看在 **Active IQ Unified Manager** 维护窗口期间生成的事件

如果需要，您可以查看在 Unified Manager 维护窗口期间为所有存储对象生成的事件。一旦维护窗口结束且所有系统资源恢复运行，大多数事件将显示为“已过时”状态。

开始之前

在任何事件可用之前，必须至少完成一个维护窗口。

默认情况下，在维护窗口期间发生的事件不会显示在事件管理清单页面上。

步骤

1. 在左侧导航窗格中，单击*事件*。

   默认情况下，所有活动（新建和已确认）事件都将显示在事件管理清单页面上。

2. 从“查看”窗格中，选择选项*维护期间生成的所有事件*。

   显示过去 7 天内从所有维护时段会话和所有群集触发的事件列表。

3. 如果单个集群有多个维护窗口，则可以单击*触发时间*日历图标，并选择您有兴趣查看的维护窗口事件的时间段。

在 **Active IQ Unified Manager** 中管理主机系统资源事件

Unified Manager 包括一项服务，用于监控安装了 Unified Manager 的主机系统上的资源问题。主机系统上缺少可用磁盘空间或内存不足等问题可能会触发管理站事件，这些事件在 UI 的顶端显示为横幅消息。

管理站事件指示安装 Unified Manager 的主机系统出现问题。管理站问题的示例包括主机系统上的磁盘空间不足；Unified Manager 缺少常规数据收集周期；以及由于启动了下一次收集轮询而导致统计分析未完成或延迟完成。

与所有其他 Unified Manager 事件消息不同，这些特定的管理站警告和关键事件显示在横幅消息中。

步骤

1. 要查看管理站事件信息，请执行以下操作：

目的	操作
查看事件详情	单击此事件横幅可显示“事件详细信息”页面，其中包含此问题的建议解决方案。
查看所有管理站事件	a. 在左侧导航窗格中，单击*事件管理*。 b. 在“事件管理清单”页面的“过滤器”窗格中，单击“源类型”列表中“管理工作站”的框。

详细了解事件

Active IQ Unified Manager 中的事件状态

事件的状态可帮助您确定是否需要采取适当的纠正措施。事件可以是“新建”、“已确认”、“已解决”或“已过时”。请注意，“新建”和“已确认”事件均被视为活动事件。

事件状态如下：

- 新增

  新事件的状态。

- 已确认

  已确认事件时的状态。

- 已解决

  事件被标记为已解决时的状态。

- 已废弃

  事件自动更正或事件原因不再有效时的状态。

  您无法确认或解决废弃的事件。

事件不同状态的示例

以下示例说明了手动和自动事件状态更改。

当触发 Cluster Not Reachable 事件时，事件状态为 New。当您确认该事件时，事件状态将变为 Acknowledged。在采取适当的纠正措施后，您必须将该事件标记为已解决。然后，事件状态将变为 Resolved。

如果由于停电而生成了 Cluster Not Reachable 事件，则在恢复供电后，群集将在没有任何管理员干预的情况下开始运行。因此，Cluster Not Reachable 事件不再有效，并且事件状态将在下一监控周期更改为 Obsolete。

当事件处于“已过时”或“已解决”状态时，Unified Manager 会发送警报。警报的电子邮件主题行和电子邮件内容提供了有关事件状态的信息。SNMP 陷阱还包含有关事件状态的信息。

了解 **Active IQ Unified Manager** 中的事件严重性类型

每个事件都与严重程度类型相关联，以帮助您对需要立即采取纠正措施的事件进行优先级排序。

- 严重

  发生了一个问题，如果不立即采取纠正措施，可能会导致服务中断。

  性能关键事件仅从用户定义的阈值发送。

- 错误

  事件源仍在运行；但是，需要采取纠正措施以避免服务中断。

- 警告

  事件源发生了您应注意的事件，或者集群对象的性能计数器超出正常范围，应进行监控以确保其未达到严重级别。此严重程度的事件不会导致服务中断，可能不需要立即采取纠正措施。

  性能警告事件从用户定义、系统定义或动态阈值发送。

- 信息

  当发现新对象或执行用户操作时，会发生此事件。例如，当删除任何存储对象或发生任何配置更改时，将生成严重性类型为“信息”的事件。

  当检测到配置更改时，信息事件将直接从 ONTAP 发送。

了解 **Active IQ Unified Manager** 中的事件影响级别

每个事件都与影响级别（突发事件、风险、事件或升级）相关联，以帮助您优先处理需要立即采取纠正措施的事件。

- 事件

  事件是一组可能导致集群停止向客户端提供数据并耗尽数据存储空间的事件。影响级别为"事件"的事件最为严重。应立即采取纠正措施，以避免服务中断。

- 风险

  风险是一组事件，这些事件可能会导致集群停止向客户端提供数据，并耗尽用于存储数据的空间。影响级别为“风险”的事件可能会导致服务中断。可能需要采取纠正措施。

- 事件

  事件是存储对象及其属性的状态或状态更改。影响级别为“事件”的事件仅供参考，无需采取纠正措施。

- 升级

  升级事件是 Active IQ 平台报告的特定类型的事件。这些事件指出的问题，其解决方案需要您升级 ONTAP 软件、节点固件或操作系统软件（针对安全公告）。您可能需要立即对其中一些问题采取纠正措施，而其他

问题则可以等到下一次计划内维护时再处理。

了解 **Active IQ Unified Manager** 中的事件影响区域

事件分为六个影响领域（可用性、容量、配置、性能、保护和安全性），使您能够专注于自己负责的事件类型。

- 可用性

  如果存储对象脱机、协议服务关闭、发生存储故障转移问题或发生硬件问题，可用性事件会通知您。

- 容量

  容量事件会通知您聚合、卷、LUN 或命名空间是否接近或已达到大小阈值，或者您的环境的增长率是否异常。

- 配置

  配置事件会通知您存储对象的发现、删除、添加、移除或重命名。配置事件的影响级别为事件，严重性类型为信息。

- 性能

  性能事件会通知您群集上的资源、配置或活动条件，这些条件可能会对受监视存储对象上的数据存储输入或检索速度产生不利影响。

- 保护

  保护事件会通知您涉及 SnapMirror 关系的事件或风险、目标容量问题、SnapVault 关系问题或保护作业问题。托管辅助卷和保护关系的任何 ONTAP 对象（特别是聚合、卷和 SVM）都归类在保护影响区域中。

- 安全

  安全事件根据 "适用于 ONTAP 9 的 NetApp 安全强化指南"中定义的参数，通知您 ONTAP 集群、存储虚拟机（SVM）和卷的安全程度。

  此外，此区域还包括 Active IQ 平台报告的升级事件。

Active IQ Unified Manager 如何计算对象状态

对象状态由当前处于“新建”或“已确认”状态的最严重事件确定。例如，如果对象状态为 Error，则对象的某个事件的严重性类型为 Error。采取纠正措施后，事件状态将变为“已解决”。

了解 **Active IQ Unified Manager** 中的动态性能事件

对于动态性能事件，“事件详细信息”页面的“系统诊断”部分列出了存在争用的集群组件延迟或使用率最高的顶级工作负载。

性能统计数据基于检测到性能事件的时间，直至上次分析事件的时间。图表还显示处于争用状态的集群组件的历史性能统计信息。

例如，您可以识别组件利用率高的工作负载，以确定将哪些工作负载转移到利用率较低的组件。移动工作负载将减少当前组件的工作量，可能使组件脱离争用状态。本节顶部是检测到事件并进行上次分析的时间和日期范围。对于活动事件（新事件或已确认事件），上次分析的时间将被更新。

将光标悬停在图表上时，延迟和活动图表会显示顶级工作负载的名称。单击图表右侧的工作负载类型菜单，您可以根据工作负载在事件中的角色（包括 *sharks* 、 *bullies* 或 *victims* ）对工作负载进行排序，并显示有关其延迟及其在争用集群组件中的使用情况的详细信息。您可以将实际值与预期值进行比较，以查看工作负载何时超出其预期的延迟或使用范围。有关信息，请参阅 "由 Unified Manager 监控的工作负载类型"。

当您按延迟的峰值偏差排序时，系统定义的工作负载不会显示在表中，因为延迟仅适用于用户定义的工作负载。具有极低延迟值的工作负载不会显示在表中。

有关动态性能阈值的详细信息，请参见 "分析动态性能阈值生成的事件"。

有关 Unified Manager 如何对工作负载进行排序和确定排序顺序的信息，请参见 "Unified Manager 如何确定事件对性能的影响"。

图表中的数据显示了上次分析事件之前的 24 小时性能统计数据。每个工作负载的实际值和预期值基于工作负载参与事件的时间。例如，工作负载可能会在检测到事件后参与事件，因此其性能统计信息可能与事件检测时的值不匹配。默认情况下，工作负载按延迟的峰值（最高）偏差进行排序。

由于 Unified Manager 最多保留 30 天的 5 分钟历史性能和事件数据，因此如果此事件是 30 多天前的，则不会显示任何性能数据。

- **Workload Sort** 列
  - 延迟图表

    显示上次分析过程中事件对工作负载延迟的影响。

  - **Component Usage** 列

    显示有关发生争用的集群组件的工作负载使用情况的详细信息。在图表中，实际使用情况显示为一条蓝线。红色条突出显示从检测时间到上次分析时间的事件持续时间。有关详细信息，请参见 "工作负载性能测量值"。

    对于网络组件，由于网络性能统计信息来自集群外的活动，因此不会显示此列。

  - 组件使用

    以百分比显示网络处理、数据处理和聚合组件的利用率历史记录，或以百分比显示 QoS 策略组组件的活动历史记录。不显示网络或互连组件的图表。您可以指向统计数据以查看特定时间点的使用统计数据。

  - 总写入 **MB/s** 历史记录

    仅对于 MetroCluster Resources 组件，显示在 MetroCluster 配置中镜像到配对集群的所有卷工作负载的总写入吞吐量，以兆字节每秒（MBps）为单位。

  - 事件历史记录

    显示红色阴影线条以指示争用组件的历史事件。对于过时的事件，图表显示在检测到所选事件之前和解决该事件之后发生的事件。

Active IQ Unified Manager 检测到的配置更改

Unified Manager 监控您的集群的配置更改，以帮助您确定更改是否可能导致或促成性能事件。性能资源管理器页面显示更改事件图标（●），以指示检测到更改的日期和时间。

您可以在“性能资源管理器”页面和“工作负载分析”页面中查看性能图表，以查看更改事件是否影响所选集群对象的性能。如果在性能事件发生的同时或前后检测到更改，则该更改可能是导致问题的原因，从而触发了事件警报。

Unified Manager 可以检测到以下变更事件，这些事件被归类为信息事件：

- 卷在聚合之间移动。

  Unified Manager 可以检测移动是正在进行、已完成还是已失败。如果 Unified Manager 在卷移动期间停止运行，则在恢复运行时，它会检测到卷移动并为其显示一个更改事件。

- 包含一个或多个受监控工作负载的 QoS 策略组的吞吐量（MB/s 或 IOPS）限制发生更改。

  更改策略组限制可能会导致延迟（响应时间）出现间歇性峰值，这也可能触发策略组的事件。延迟会逐渐恢复正常，由峰值引起的任何事件都会过时。

- HA 对中的节点接管或交还其伙伴节点的存储。

  Unified Manager 可以检测接管、部分接管或交还操作何时完成。如果接管是由崩溃的节点引起的，则 Unified Manager 不会检测到该事件。

- 已成功完成 ONTAP 升级或还原操作。

  将显示先前版本和新版本。

事件和严重性类型列表

了解 **Active IQ Unified Manager** 中的聚合事件

聚合事件可为您提供有关聚合状态的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

事件名称（陷阱名称）	影响级别	源类型	严重性
聚合离线（ocumEvtAggregateStateOffline）	意外事件	聚合	关键
聚合失败（ocumEvtAggregateStateFailed）	意外事件	聚合	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
聚合受限（ocumEvtAggregateStateRestricted）	风险	聚合	警告
聚合重建（ocumEvtAggregateRaidStateReconstructing）	风险	聚合	警告
聚合已降级（ocumEvtAggregateRaidStateDegraded）	风险	聚合	警告
云层可部分访问（ocumEventCloudTierPartiallyReachable）	风险	聚合	警告
云层无法访问（ocumEventCloudTierUnreachable）	风险	聚合	错误
用于聚合重新定位的云层访问被拒绝*（arlNetraCaCheckFailed）	风险	聚合	错误
存储故障转移期间用于聚合重新定位的云层访问被拒绝 *（gbNetraCaCheckFailed）	风险	聚合	错误
MetroCluster 聚合遗留（ocumEvtMetroClusterAggregateLeftBehind）	风险	聚合	错误
MetroCluster 聚合镜像已降级（ocumEvtMetroClusterAggregateMirrorDegraded）	风险	聚合	错误

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
聚合空间接近全满（ocumEvtAggregateNearlyFull）	风险	聚合	警告
聚合空间全满（ocumEvtAggregateFull）	风险	聚合	错误
聚合达到全满前的天数（ocumEvtAggregateDaysUntilFullSoon）	风险	聚合	错误

事件名称（陷阱名称）	影响级别	源类型	严重性
聚合过度配置（ocumEvtAggregateOvercommitted）	风险	聚合	错误
聚合接近过量提交（ocumEvtAggregateAlmostOvercommitted）	风险	聚合	警告
聚合 Snapshot 预留满（ocumEvtAggregateSnapReserveFull）	风险	聚合	警告
聚合增长率异常（ocumEvtAggregateGrowthRateAbnormal）	风险	聚合	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
已发现聚合（不适用）	事件	聚合	信息
聚合已重命名（不适用）	事件	聚合	信息
聚合已删除（不适用）	事件	节点	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反聚合 IOPS 严重阈值（ocumAggregateIopsIncident）	意外事件	聚合	关键
已违反聚合 IOPS 警告阈值（ocumAggregateIopsWarning）	风险	聚合	警告
已违反聚合 MB/s 严重阈值（ocumAggregateMbpsIncident）	意外事件	聚合	关键
已违反聚合 MB/s 警告阈值（ocumAggregateMbpsWarning）	风险	聚合	警告
已违反聚合延迟严重阈值（ocumAggregateLatencyIncident）	意外事件	聚合	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反聚合延迟警告阈值（ocumAggregateLatencyWarning）	风险	聚合	警告
已违反已用聚合性能容量严重阈值（ocumAggregatePerfCapacityUsedIncident）	意外事件	聚合	关键
已违反聚合已用性能容量警告阈值（ocumAggregatePerfCapacityUsedWarning）	风险	聚合	警告
已违反聚合利用率严重阈值（ocumAggregateUtilizationIncident）	意外事件	聚合	关键
已违反聚合利用率警告阈值（ocumAggregateUtilizationWarning）	风险	聚合	警告
已违反聚合磁盘过度利用阈值（ocumAggregateDisksOverUtilizedWarning）	风险	聚合	警告
已违反聚合动态阈值（ocumAggregateDynamicEventWarning）	风险	聚合	警告

了解 **Active IQ Unified Manager** 中的集群事件

集群事件提供了有关集群状态的信息，可用于监控集群中的潜在问题。事件按影响区域进行分组，且包括事件名称、陷阱名称、影响级别、源类型和严重性。

影响区域：可用性

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

事件名称（陷阱名称）	影响级别	源类型	严重性
集群缺少备用磁盘（ocumEvtDisksNoSpares）	风险	集群	警告
集群无法访问（ocumEvtClusterUnreachable）	风险	集群	错误
集群监控失败（ocumEvtClusterMonitoringFailed）	风险	集群	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反集群 FabricPool 许可证容量限制（ocumEvtExternalCapacityTierSpaceFull）	风险	集群	警告
NVMe-oF 宽限期已开始 *（nvmfGracePeriodStart）	风险	集群	警告
NVMe-oF 宽限期处于活动状态 *(nvmfGracePeriodActive)	风险	集群	警告
NVMe-oF 宽限期已过期 *（nvmfGracePeriodExpired）	风险	集群	警告
对象维护窗口已启动（objectMaintenanceWindowStarted）	事件	集群	关键
对象维护窗口已结束（objectMaintenanceWindowEnded）	事件	集群	信息
MetroCluster 备用磁盘遗留（ocumEvtSpareDiskLeftBehind）	风险	集群	错误
MetroCluster 自动计划外切换已禁用（ocumEvtMccAutomaticUnplannedSwitchOverDisabled）	风险	集群	警告
集群用户密码已更改 *（cluster.passwd.changed）	事件	集群	信息

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
已超过集群容量不平衡阈值（ocumConformanceNodeImbalanceWarning）	风险	集群	警告
集群云层规划（clusterCloudTierPlanningWarning）	风险	集群	警告
FabricPool 镜像复制重新同步已完成 *（waflCaResyncComplete）	事件	集群	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
FabricPool 空间接近全满 *（fabricpoolNearlyFull）	风险	集群	错误

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
已添加节点（不适用）	事件	集群	信息
节点已删除（不适用）	事件	集群	信息
群集已删除（不适用）	事件	集群	信息
集群添加失败（不适用）	事件	集群	错误
集群名称已更改（不适用）	事件	集群	信息
收到紧急 EMS（不适用）	事件	集群	关键
收到严重 EMS（不适用）	事件	集群	关键
收到 EMS 警报（不适用）	事件	集群	错误
收到 EMS 错误（不适用）	事件	集群	警告
收到 EMS 警告（不适用）	事件	集群	警告
收到调试 EMS（不适用）	事件	集群	警告
收到 EMS 通知（不适用）	事件	集群	警告
收到信息性 EMS（不适用）	事件	集群	警告

ONTAP EMS 事件分为三个 Unified Manager 事件严重性级别。

Unified Manager 事件严重性级别	ONTAP EMS 事件严重性级别
关键	紧急 关键
错误	警报
警告	错误 警告 调试 通知 信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已超出集群负载不平衡阈值（）	风险	集群	警告
已违反集群 IOPS 严重阈值（ocumClusterIopsIncident）	意外事件	集群	关键
已违反集群 IOPS 警告阈值（ocumClusterIopsWarning）	风险	集群	警告
已违反集群 MB/s 严重阈值（ocumClusterMbpsIncident）	意外事件	集群	关键
已违反集群 MB/s 警告阈值（ocumClusterMbpsWarning）	风险	集群	警告
已违反集群动态阈值（ocumClusterDynamicEventWarning）	风险	集群	警告

影响区域：安全性

事件名称（陷阱名称）	影响级别	源类型	严重性
AutoSupport HTTPS传输已禁用（ocumClusterASUPHttpsConfiguredDisabled）	风险	集群	警告
日志转发未加密（ocumClusterAuditLogUnencrypted）	风险	集群	警告
已启用默认本地管理员用户（ocumClusterDefaultAdminEnabled）	风险	集群	警告
已禁用 FIPS 模式（ocumClusterFipsDisabled）	风险	集群	警告
已禁用登录横幅（ocumClusterLoginBannerDisabled）	风险	集群	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
登录横幅已更改（ocumClusterLoginBannerChanged）	风险	集群	警告
日志转发目标已更改（ocumLogForwardDestinationsChanged）	风险	集群	警告
NTP 服务器名称已更改（ocumNtpServerNamesChanged）	风险	集群	警告
NTP服务器计数低（securityConfigNTPServerCountLowRisk）	风险	集群	警告
集群对等通信未加密（ocumClusterPeerEncryptionDisabled）	风险	集群	警告
SSH正在使用不安全密码（ocumClusterSSHInsecure）	风险	集群	警告
Telnet 协议已启用（ocumClusterTelnetEnabled）	风险	集群	警告
某些 ONTAP 用户帐户的密码使用不太安全的 MD5 哈希函数（ocumClusterMD5PasswordHashUsed）	风险	集群	警告
群集使用自签名证书（ocumClusterSelfSignedCertificate）	风险	集群	警告
集群远程 Shell 已启用（ocumClusterRshDisabled）	风险	集群	警告
群集证书即将过期（ocumEvtClusterCertificateAboutToExpire）	风险	集群	警告
群集证书已过期（ocumEvtClusterCertificateExpired）	风险	集群	错误

了解 **Active IQ Unified Manager** 中的磁盘事件

磁盘事件为您提供有关磁盘状态的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
闪存磁盘 - 几乎用尽备用数据块（ocumEvtClusterFlashDiskFewerSpareBlockError）	风险	集群	错误
闪存磁盘 - 无备用数据块（ocumEvtClusterFlashDiskNoSpareBlockCritical）	意外事件	集群	关键
一些未分配的磁盘（ocumEvtClusterUnassignedDisksSome）	风险	集群	警告
部分故障磁盘（ocumEvtDisksSomeFailed）	意外事件	集群	关键

了解 **Active IQ Unified Manager** 中的机柜事件

机箱事件可为您提供有关数据中心中磁盘架机箱状态的信息，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
磁盘架风扇出现故障（ocumEvtShelfFanFailed）	意外事件	存储架	关键
磁盘架电源出现故障（ocumEvtShelfPowerSupplyFailed）	意外事件	存储架	关键
未配置磁盘架多路径（ocumDiskShelfConnectivityNotInMultiPath） 此事件不适用于： • 处于 MetroCluster 配置中的集群 • 以下平台：FAS2554、FAS2552、FAS2520 和 FAS2240	风险	节点	警告
磁盘架路径故障（ocumDiskShelfConnectivityPathFailure）	风险	存储架	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
已发现磁盘架（不适用）	事件	节点	信息
已移除磁盘架（不适用）	事件	节点	信息

了解 **Active IQ Unified Manager** 中的风扇事件

风扇事件为您提供有关数据中心内节点上风扇状态的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
一个或多个风扇出现故障（ocumEvtFansOneOrMoreFailed）	意外事件	节点	关键

了解 **Active IQ Unified Manager** 中的闪存卡事件

闪存卡事件为您提供有关安装在数据中心节点上的闪存卡状态的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
闪存卡离线（ocumEvtFlashCardOffline）	意外事件	节点	关键

了解 **Active IQ Unified Manager** 中的 **inode** 事件

当 inode 已满或接近已满时，inode 事件会提供相关信息，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型以及严重性。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
索引节点接近全满（ocumEvtInodesAlmostFull）	风险	卷	警告
Inodes Full（ocumEvtInodesFull）	风险	卷	错误

Active IQ Unified Manager 中的网络接口事件

网络接口事件提供有关网络接口（LIF）状态的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
网络接口状态已关闭（ocumEvtLifStatusDown）	风险	接口	错误
FC/FCoE 网络接口状态已关闭（ocumEvtFCLifStatusDown）	风险	接口	错误
无法进行网络接口故障转移（ocumEvtLifFailoverNotPossible）	风险	接口	警告
网络接口不位于主端口（ocumEvtLifNotAtHomePort）	风险	接口	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
网络接口路由未配置（不适用）	事件	接口	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反网络接口 MB/s 严重阈值（ocumNetworkLifMbpsIncident）	意外事件	接口	关键
已违反网络接口 MB/s 警告阈值（ocumNetworkLifMbpsWarning）	风险	接口	警告
已违反 FC 网络接口 MB/s 严重阈值（ocumFcpLifMbpsIncident）	意外事件	接口	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反 FC 网络接口 MB/s 警告阈值（ocumFcpLifMbpsWarning）	风险	接口	警告
已违反 NVMf FC 网络接口 MB/s 严重阈值（ocumNvmfFcLifMbpsIncident）	意外事件	接口	关键
已违反 NVMf FC 网络接口 MB/s 警告阈值（ocumNvmfFcLifMbpsWarning）	风险	接口	警告

了解 **Active IQ Unified Manager** 中的 **LUN** 事件

LUN 事件可为您提供有关 LUN 状态的信息，以便您可以监视潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

事件名称（陷阱名称）	影响级别	源类型	严重性
LUN 离线（ocumEvtLunOffline）	意外事件	LUN	关键
LUN 已销毁 *（lunDestroy）	事件	LUN	信息
igroup 中映射了不受支持的操作系统的 LUN（igroupUnsupportedOsType）	意外事件	LUN	警告
访问 LUN 的单一活动路径（ocumEvtLunSingleActivePath）	风险	LUN	警告
没有可访问 LUN 的活动路径（ocumEvtLunNotReachable）	意外事件	LUN	关键
没有可访问 LUN 的优化路径（ocumEvtLunOptimizedPathInactive）	风险	LUN	警告
没有可从 HA 配对节点（ocumEvtLunHaPathInactive）访问 LUN 的路径	风险	LUN	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
无路径可从 HA 对中的一个节点访问 LUN（ocumEvtLunNodePathStatusDown）	风险	LUN	错误

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
LUN Snapshot 副本的空间不足（ocumEvtLunSnapshotNotPossible）	风险	卷	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
igroup 中映射了不受支持的操作系统的 LUN（igroupUnsupportedOsType）	风险	LUN	警告

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反 LUN IOPS 严重阈值（ocumLunIopsIncident）	意外事件	LUN	关键
已违反 LUN IOPS 警告阈值（ocumLunIopsWarning）	风险	LUN	警告
已违反 LUN MB/s 严重阈值（ocumLunMbpsIncident）	意外事件	LUN	关键
已违反 LUN MB/秒警告阈值（ocumLunMbpsWarning）	风险	LUN	警告
已违反 LUN 延迟（毫秒/操作）关键阈值（ocumLunLatencyIncident）	意外事件	LUN	关键
已违反 LUN 延迟毫秒/操作警告阈值（ocumLunLatencyWarning）	风险	LUN	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反 LUN 延迟和 IOPS 严重阈值（ocumLunLatencyIopsIncident）	意外事件	LUN	关键
已违反 LUN 延迟和 IOPS 警告阈值（ocumLunLatencyIopsWarning）	风险	LUN	警告
已违反 LUN 延迟和 MB/s 严重阈值（ocumLunLatencyMbpsIncident）	意外事件	LUN	关键
已违反 LUN 延迟和 MB/s 警告阈值（ocumLunLatencyMbpsWarning）	风险	LUN	警告
已违反 LUN 延迟和聚合已用性能容量严重阈值（ocumLunLatencyAggregatePerfCapacityUsedIncident）	意外事件	LUN	关键
已违反 LUN 延迟和聚合已用性能容量警告阈值（ocumLunLatencyAggregatePerfCapacityUsedWarning）	风险	LUN	警告
已违反 LUN 延迟和聚合利用率严重阈值（ocumLunLatencyAggregateUtilizationIncident）	意外事件	LUN	关键
LUN 延迟和聚合利用率警告阈值已违反（ocumLunLatencyAggregateUtilizationWarning）	风险	LUN	警告
已违反 LUN 延迟和节点已用性能容量严重阈值（ocumLunLatencyNodePerfCapacityUsedIncident）	意外事件	LUN	关键
已违反 LUN 延迟和节点已用性能容量警告阈值（ocumLunLatencyNodePerfCapacityUsedWarning）	风险	LUN	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
LUN 延迟和已用节点性能容量 - 已违反接管严重阈值（ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident）	意外事件	LUN	关键
LUN 延迟和已用节点性能容量 - 已违反接管警告阈值（ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning）	风险	LUN	警告
已违反 LUN 延迟和节点利用率严重阈值（ocumLunLatencyNodeUtilizationIncident）	意外事件	LUN	关键
已违反 LUN 延迟和节点利用率警告阈值（ocumLunLatencyNodeUtilizationWarning）	风险	LUN	警告
已违反 QoS LUN 最大 IOPS 警告阈值（ocumQosLunMaxIopsWarning）	风险	LUN	警告
已违反 QoS LUN 最大 MB/s 警告阈值（ocumQosLunMaxMbpsWarning）	风险	LUN	警告
已违反性能服务级别策略定义的工作负载 LUN 延迟阈值（ocumConformanceLatencyWarning）	风险	LUN	警告

了解 **Active IQ Unified Manager** 中的管理站事件

管理站事件可为您提供有关安装了 Unified Manager 的服务器状态的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
管理服务器磁盘空间接近全满（ocumEvtUnifiedManagerDiskSpaceNearlyFull）	风险	管理站	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
管理服务器磁盘空间已满（ocumEvtUnifiedManagerDiskSpaceFull）	意外事件	管理站	关键
管理服务器内存不足（ocumEvtUnifiedManagerMemoryLow）	风险	管理站	警告
管理服务器内存几乎用尽（ocumEvtUnifiedManagerMemoryAlmostOut）	意外事件	管理站	关键
MySQL 日志文件大小已增加；需要重新启动（ocumEvtMysqlLogFileSizeWarning）	意外事件	管理站	警告
审核日志总大小分配即将满	风险	管理站	警告
Syslog 服务器证书即将过期	风险	管理站	警告
Syslog 服务器证书已过期	风险	管理站	错误
审核日志文件已篡改	风险	管理站	警告
审核日志文件已删除	风险	管理站	警告
Syslog 服务器连接错误	风险	管理站	错误
Syslog 服务器配置已更改	事件	管理站	警告

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
性能数据分析受影响（ocumEvtUnifiedManagerDataMissingAnalyze）	风险	管理站	警告
性能数据收集受影响（ocumEvtUnifiedManagerDataMissingCollection）	意外事件	管理站	关键

最后两个性能事件仅适用于 Unified Manager 7.2。如果这些事件中的任何一个处于“新建”状态，然后您升级到较新版本的 Unified Manager 软件，则不会自动清除这些事件。您需要手动将事件移至“已解决”状态。

了解 **Active IQ Unified Manager** 中的 **MetroCluster Bridge** 事件

MetroCluster 网桥事件为您提供有关网桥状态的信息，以便您可以监控 MetroCluster over FC 配置中的潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
网桥不可达（ocumEvtBridgeUnreachable）	意外事件	MetroCluster 桥接	关键
桥温异常（ocumEvtBridgeTemperatureAbnormal）	意外事件	MetroCluster 桥接	关键

了解 **Active IQ Unified Manager** 中的 **MetroCluster** 连接事件

连接事件为您提供有关群集组件之间以及基于 FC 的 MetroCluster 和基于 IP 的 MetroCluster 配置中群集之间连接的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重程度。

两种配置中常见的事件

这些连接事件在基于 FC 的 MetroCluster 和基于 IP 的 MetroCluster 配置中都很常见。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
MetroCluster 伙伴之间的所有链路均已关闭（ocumEvtMetroClusterAllLinksBetweenPartnersDown）	意外事件	MetroCluster 关系	关键
MetroCluster 无法通过对等网络访问配对集群（ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork）	意外事件	MetroCluster 关系	关键
MetroCluster 灾难恢复功能受影响（ocumEvtMetroClusterDRStatusImpacted）	风险	MetroCluster 关系	关键
MetroCluster 配置已切换（ocumEvtMetroClusterDRStatusImpacted）	风险	MetroCluster 关系	警告

MetroCluster 基于 **FC** 的配置

这些事件与基于 FC 的 MetroCluster 配置有关。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
所有交换机间链路已关闭（ocumEvtMetroClusterAllISLBetweenSwitchesDown）	意外事件	MetroCluster 交换机间连接	关键
FC-SAS 网桥到存储堆栈的链路已关闭（ocumEvtBridgeSasPortDown）	意外事件	MetroCluster 网桥堆栈连接	关键
MetroCluster 配置已部分切换（ocumEvtMetroClusterDRStatusPartiallyImpacted）	风险	MetroCluster 关系	错误
节点到 FC 交换机的所有 FC-VI 互连链路已关闭（ocumEvtMccNodeSwitchFcviLinksDown）	意外事件	MetroCluster 节点交换机连接	关键
节点到 FC 交换机的一个或多个 FC 启动器链路已关闭（ocumEvtMccNodeSwitchFcLinksOneOrMoreDown）	风险	MetroCluster 节点交换机连接	警告
节点到 FC 交换机所有 FC 启动程序链路断开（ocumEvtMccNodeSwitchFcLinksDown）	意外事件	MetroCluster 节点交换机连接	关键
交换机到 FC-SAS 网桥的 FC 链路已关闭（ocumEvtMccSwitchBridgeFcLinksDown）	意外事件	MetroCluster 交换机网桥连接	关键
Inter Node All FC VI InterConnect 链路全部断开(ocumEvtMccInterNodeLinksDown)	意外事件	节点间连接	关键
节点间的一个或多个 FC VI InterConnect 链路已关闭（ocumEvtMccInterNodeLinksOneOrMoreDown）	风险	节点间连接	警告
节点到网桥的链路已关闭（ocumEvtMccNodeBridgeLinksDown）	意外事件	节点网桥连接	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
节点到存储堆栈的所有 SAS 链路已关闭（ocumEvtMccNodeStackLinksDown）	意外事件	节点堆栈连接	关键
节点到存储堆栈的一个或多个 SAS 链路已关闭（ocumEvtMccNodeStackLinksOneOrMoreDown）	风险	节点堆栈连接	警告

基于 **IP** 的 **MetroCluster** 配置

这些事件涉及基于 IP 的 MetroCluster 配置。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
MetroCluster IP 站点间连接状态为已关闭（mccIntersiteconnectivityStatusDown）	风险	MetroCluster 关系	关键
MetroCluster-IP 节点到交换机连接离线（mccIpPortStatusOffline）	风险	节点	错误

了解 **Active IQ Unified Manager** 中的 **MetroCluster** 交换机事件

针对基于 FC 的 MetroCluster 配置的 MetroCluster 交换机事件可为您提供有关 MetroCluster 交换机状态的信息，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
交换机温度异常（ocumEvtSwitchTemperatureAbnormal）	意外事件	MetroCluster 交换机	关键
交换机无法访问（ocumEvtSwitchUnreachable）	意外事件	MetroCluster 交换机	关键
交换机风扇出现故障（ocumEvtSwitchFansOneOrMoreFailed）	意外事件	MetroCluster 交换机	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
交换机电源出现故障（ocumEvtSwitchPowerSuppliesOneOrMoreFailed）	意外事件	MetroCluster 交换机	关键
交换机温度传感器出现故障（ocumEvtSwitchTemperatureSensorFailed） 此事件仅适用于 Cisco 交换机。	意外事件	MetroCluster 交换机	关键

了解 **Active IQ Unified Manager** 中的 **NVMe** 命名空间事件

NVMe 命名空间事件可为您提供有关命名空间状态的信息，以便您可以监视潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
NVMeNS 离线 *（nvmeNamespaceStatusOffline）	事件	命名空间	信息
NVMeNS 在线 *(nvmeNamespaceStatusOnline)	事件	命名空间	信息
NVMeNS 空间不足 *（nvmeNamespaceSpaceOutOfSpace）	风险	命名空间	警告
NVMeNS 销毁 *（nvmeNamespaceDestroy）	事件	命名空间	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
NVMe 命名空间 IOPS 严重阈值已突破（ocumNvmeNamespaceIopsIncident）	意外事件	命名空间	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反 NVMe 命名空间 IOPS 警告阈值（ocumNvmeNamespaceIopsWarning）	风险	命名空间	警告
NVMe 命名空间 MB/s 严重阈值已超出（ocumNvmeNamespaceMbpsIncident）	意外事件	命名空间	关键
已违反 NVMe 命名空间 MB/s 警告阈值（ocumNvmeNamespaceMbpsWarning）	风险	命名空间	警告
NVMe 命名空间延迟 ms/op 严重阈值已违反（ocumNvmeNamespaceLatencyIncident）	意外事件	命名空间	关键
已违反 NVMe 命名空间延迟 ms/op 警告阈值（ocumNvmeNamespaceLatencyWarning）	风险	命名空间	警告
已违反 NVMe 命名空间延迟和 IOPS 严重阈值（ocumNvmeNamespaceLatencyIopsIncident）	意外事件	命名空间	关键
已违反 NVMe 命名空间延迟和 IOPS 警告阈值（ocumNvmeNamespaceLatencyIopsWarning）	风险	命名空间	警告
已违反 NVMe 命名空间延迟和 MB/s 严重阈值（ocumNvmeNamespaceLatencyMbpsIncident）	意外事件	命名空间	关键
已违反 NVMe 命名空间延迟和 MB/s 警告阈值（ocumNvmeNamespaceLatencyMbpsWarning）	风险	命名空间	警告

了解 **Active IQ Unified Manager** 中的节点事件

节点事件提供了有关节点状态的信息，可用于监控潜在的问题。事件按影响区域进行分组，并可提供事件和陷阱名称、影响级别、源类型和严重性。

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
节点根卷空间即将满（ocumEvtClusterNodeRootVolumeSpaceNearlyFull）	风险	节点	警告
Cloud AWS MetaDataConnFail *（ocumCloudAwsMetadataConnFail）	风险	节点	错误
云 AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	风险	节点	错误
云 AWS IAMCredsInvalid *（ocumCloudAwsIamCredsInvalid）	风险	节点	错误
云 AWS IAMCredsNotFound *（ocumCloudAwsIamCredsNotFound）	风险	节点	错误
云 AWS IAMCredsNotInitialized *（ocumCloudAwsIamCredsNotInitialized）	事件	节点	信息
云 AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	风险	节点	错误
云 AWS IAMRoleNotFound *（ocumCloudAwsIamRoleNotFound）	风险	节点	错误
云层主机无法解析 *（ocumObjstoreHostUnresolvable）	风险	节点	错误
云层集群间网络接口已关闭 *（ocumObjstoreInterClusterLifDown）	风险	节点	错误
其中一个 NFSv4 池已耗尽 *（nbladeNfsv4PoolEXhaust）	意外事件	节点	关键
请求与云分层签名不匹配 *(oscSignatureMismatch)	风险	节点	错误

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
QoS Monitor 内存已达上限 *（ocumQosMonitorMemoryMaxed）	风险	节点	错误
QoS 监控内存已缩减 *（ocumQosMonitorMemoryAbated）	事件	节点	信息

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
节点已重命名（不适用）	事件	节点	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反节点 IOPS 严重阈值（ocumNodeIopsIncident）	意外事件	节点	关键
已违反节点 IOPS 警告阈值（ocumNodeIopsWarning）	风险	节点	警告
节点 MB/s 严重阈值已违反（ocumNodeMbpsIncident）	意外事件	节点	关键
已违反节点 MB/s 警告阈值（ocumNodeMbpsWarning）	风险	节点	警告
已违反节点延迟毫秒/操作严重阈值（ocumNodeLatencyIncident）	意外事件	节点	关键
已违反节点延迟毫秒/操作警告阈值（ocumNodeLatencyWarning）	风险	节点	警告
违反节点已用性能容量严重阈值（ocumNodePerfCapacityUsedIncident）	意外事件	节点	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反节点已用性能容量警告阈值（ocumNodePerfCapacityUsedWarning）	风险	节点	警告
已用节点性能容量 - 已违反接管严重阈值（ocumNodePerfCapacityUsedTakeoverIncident）	意外事件	节点	关键
已用节点性能容量 - 已违反接管警告阈值（ocumNodePerfCapacityUsedTakeoverWarning）	风险	节点	警告
已违反节点利用率严重阈值（ocumNodeUtilizationIncident）	意外事件	节点	关键
已违反节点利用率警告阈值（ocumNodeUtilizationWarning）	风险	节点	警告
已违反节点 HA 对过度利用阈值（ocumNodeHaPairOverUtilizedInformation）	事件	节点	信息
已违反节点磁盘碎片化阈值（ocumNodeDiskFragmentationWarning）	风险	节点	警告
已违反已用性能容量阈值（ocumNodeOverUtilizedWarning）	风险	节点	警告
已违反节点动态阈值（ocumNodeDynamicEventWarning）	风险	节点	警告

影响区域：安全性

事件名称（陷阱名称）	影响级别	源类型	严重性
咨询 ID：NTAP-<*advisory ID*>（ocumx）	风险	节点	关键

了解 **Active IQ Unified Manager** 中的 **NVRAM** 电池事件

NVRAM 电池事件可为您提供有关电池状态的信息，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
NVRAM 电池电量低（ocumEvtNvramBatteryLow）	风险	节点	警告
NVRAM 电池已放电（ocumEvtNvramBatteryDischarged）	风险	节点	错误
NVRAM 电池充电过度（ocumEvtNvramBatteryOverCharged）	意外事件	节点	关键

了解 **Active IQ Unified Manager** 中的端口事件

端口事件为您提供有关集群端口的状态，以便您可以监控端口上的更改或问题，例如端口是否已关闭。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
端口状态已关闭（ocumEvtPortStatusDown）	意外事件	节点	关键

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反网络端口 MB/s 严重阈值（ocumNetworkPortMbpsIncident）	意外事件	端口	关键
已违反网络端口 MB/s 警告阈值（ocumNetworkPortMbpsWarning）	风险	端口	警告
已违反 FCP 端口 MB/s 严重阈值（ocumFcpPortMbpsIncident）	意外事件	端口	关键
已违反 FCP 端口 MB/s 警告阈值（ocumFcpPortMbpsWarning）	风险	端口	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反网络端口利用率严重阈值（ocumNetworkPortUtilizationIncident）	意外事件	端口	关键
已违反网络端口利用率警告阈值（ocumNetworkPortUtilizationWarning）	风险	端口	警告
已违反 FCP 端口利用率严重阈值（ocumFcpPortUtilizationIncident）	意外事件	端口	关键
FCP 端口利用率警告阈值已违反（ocumFcpPortUtilizationWarning）	风险	端口	警告

了解 **Active IQ Unified Manager** 中的电源事件

电源事件可为您提供有关硬件状态的信息，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
一个或多个电源出现故障（ocumEvtPowerSupplyOneOrMoreFailed）	意外事件	节点	关键

了解 **Active IQ Unified Manager** 中的保护事件

保护事件会告诉您作业是否已失败或中止，以便您可以监控问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：保护

事件名称（陷阱名称）	影响级别	源类型	严重性
保护作业失败（ocumEvtProtectionJobTaskFailed）	意外事件	卷或存储服务	关键
保护作业已中止（ocumEvtProtectionJobAborted）	风险	卷或存储服务	警告

了解 **Active IQ Unified Manager** 中的 **Qtree** 事件

Qtree 事件为您提供有关 qtree 容量以及文件和磁盘限制的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
Qtree 空间接近全满（ocumEvtQtreeSpaceNearlyFull）	风险	qtree	警告
Qtree 空间已满（ocumEvtQtreeSpaceFull）	风险	qtree	错误
Qtree 空间正常（ocumEvtQtreeSpaceThresholdOk）	事件	qtree	信息
已达到 Qtree 文件硬限制（ocumEvtQtreeFilesHardLimitReached）	意外事件	qtree	关键
已违反 Qtree 文件软限制（ocumEvtQtreeFilesSoftLimitBreached）	风险	qtree	警告
已达到 Qtree 空间硬限制（ocumEvtQtreeSpaceHardLimitReached）	意外事件	qtree	关键
已违反 qtree 空间软限制（ocumEvtQtreeSpaceSoftLimitBreached）	风险	qtree	警告

了解 **Active IQ Unified Manager** 中的 **Service Processor** 事件

服务处理器事件为您提供有关处理器状态的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
服务处理器未配置（ocumEvtServiceProcessorNotConfigured）	风险	节点	警告
服务处理器离线（ocumEvtServiceProcessorOffline）	风险	节点	错误

了解 **Active IQ Unified Manager** 中的 **SnapMirror** 关系事件

SnapMirror 关系事件为您提供有关异步和同步 SnapMirror 关系状态的信息，以便您可以监控潜在问题。异步 SnapMirror 关系事件是为 Storage VM 和卷生成的，而同步 SnapMirror 关系事件仅为卷关系生成。不会为属于 Storage VM 灾难恢复关系的组成卷生成任何事件。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重程度。

影响区域：保护

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

SnapMirror 关系事件是为受 Storage VM 灾难恢复保护的 Storage VM 生成的，但不会为任何组成对象关系生成。

事件名称（陷阱名称）	影响级别	源类型	严重性
镜像复制运行不正常（ocumEvtSnapmirrorRelationshipUnhealthy）	风险	SnapMirror 关系	警告
镜像复制已断开（ocumEvtSnapmirrorRelationshipStateBrokenoff）	风险	SnapMirror 关系	错误
镜像复制初始化失败（ocumEvtSnapmirrorRelationshipInitializeFailed）	风险	SnapMirror 关系	错误
镜像复制更新失败（ocumEvtSnapmirrorRelationshipUpdateFailed）	风险	SnapMirror 关系	错误
镜像复制滞后错误（ocumEvtSnapMirrorRelationshipLagError）	风险	SnapMirror 关系	错误
镜像复制滞后警告（ocumEvtSnapMirrorRelationshipLagWarning）	风险	SnapMirror 关系	警告
镜像复制重新同步失败（ocumEvtSnapmirrorRelationshipResyncFailed）	风险	SnapMirror 关系	错误
同步复制未同步 *（syncSnapmirrorRelationshipOutofsync）	风险	SnapMirror 关系	警告
同步复制已还原 *（syncSnapmirrorRelationshipInSync）	事件	SnapMirror 关系	信息

事件名称（陷阱名称）	影响级别	源类型	严重性
同步复制自动重新同步失败*（syncSnapmirrorRelationshipAutoSyncRetryFailed）	风险	SnapMirror 关系	错误
在集群（snapmirrorMediatorAdded）上添加了 Ontap Mediator	事件	集群	信息
已从集群中删除 Ontap Mediator（snapmirrorMediatorRemoved）	事件	集群	信息
无法从集群访问 Ontap Mediator（snapmirrorMediatorUnreachable）	风险	调解器	警告
无法从集群访问 Ontap Mediator（snapmirrorMediatorMisconfigured）	风险	调解器	错误
Ontap Mediator 连接已重新建立，并且已重新同步，准备好进行 SnapMirror 活动同步（snapmirrorMediatorInQuorum）	事件	调解器	信息

了解 **Active IQ Unified Manager** 中的异步镜像和 **Vault** 关系事件

异步镜像和 Vault 关系事件为您提供有关异步 SnapMirror 和 Vault 关系状态的信息，以便您可以监控潜在问题。卷和 Storage VM 保护关系均支持异步镜像和 Vault 关系事件。但是，只有 Vault 关系不支持 Storage VM 灾难恢复。事件按影响区域分组，包括事件和 trap 名称、影响级别、源类型和严重程度。

影响区域：保护

还会为受 Storage VM 灾难恢复保护的 Storage VM 生成 SnapMirror 和 Vault 关系事件，但不会为任何组成对象关系生成。

事件名称（陷阱名称）	影响级别	源类型	严重性
异步镜像和存储不正常（ocumEvtMirrorVaultRelationshipUnhealthy）	风险	SnapMirror 关系	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
异步镜像和保管库已断开（ocumEvtMirrorVaultRelationshipStateBrokenoff）	风险	SnapMirror 关系	错误
异步镜像和存储库初始化失败（ocumEvtMirrorVaultRelationshipInitializeFailed）	风险	SnapMirror 关系	错误
异步镜像和存储更新失败（ocumEvtMirrorVaultRelationshipUpdateFailed）	风险	SnapMirror 关系	错误
异步镜像和存储滞后错误（ocumEvtMirrorVaultRelationshipLagError）	风险	SnapMirror 关系	错误
异步镜像和存储滞后警告（ocumEvtMirrorVaultRelationshipLagWarning）	风险	SnapMirror 关系	警告
异步镜像和存储库重新同步失败（ocumEvtMirrorVaultRelationshipResyncFailed）	风险	SnapMirror 关系	错误

"SnapMirror 更新失败"事件由 Active IQ 门户（Config Advisor）引发。

了解 **Active IQ Unified Manager** 中的 **Snapshot** 事件

快照事件提供有关快照状态的信息，使您能够监控快照以发现潜在问题。事件按影响区域分组，包括事件名称、陷阱名称、影响级别、源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
快照自动删除已禁用（不适用）	事件	卷	信息
已启用快照自动删除（不适用）	事件	卷	信息
快照自动删除配置已修改（不适用）	事件	卷	信息

了解 **Active IQ Unified Manager** 中的 **SnapVault** 关系事件

SnapVault 关系事件可为您提供有关 SnapVault 关系状态的信息，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：保护

事件名称（陷阱名称）	影响级别	源类型	严重性
异步 Vault 不正常（ocumEvtSnapVaultRelationshipUnhealthy）	风险	SnapMirror 关系	警告
异步 Vault 已断开（ocumEvtSnapVaultRelationshipStateBrokenoff）	风险	SnapMirror 关系	错误
异步 Vault 初始化失败（ocumEvtSnapVaultRelationshipInitializeFailed）	风险	SnapMirror 关系	错误
异步 Vault 更新失败（ocumEvtSnapVaultRelationshipUpdateFailed）	风险	SnapMirror 关系	错误
异步 Vault 滞后错误（ocumEvtSnapVaultRelationshipLagError）	风险	SnapMirror 关系	错误
异步 Vault 滞后警告（ocumEvtSnapVaultRelationshipLagWarning）	风险	SnapMirror 关系	警告
异步 Vault 重新同步失败（ocumEvtSnapvaultRelationshipResyncFailed）	风险	SnapMirror 关系	错误

了解 **Active IQ Unified Manager** 中的存储故障转移设置事件

存储故障转移（SFO）设置事件可为您提供有关存储故障转移是否已禁用或未配置的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
存储故障转移互连一个或多个链路已关闭（ocumEvtSfoInterconnectOneOrMoreLinksDown）	风险	节点	警告
存储故障转移已禁用（ocumEvtSfoSettingsDisabled）	风险	节点	错误
未配置存储故障转移（ocumEvtSfoSettingsNotConfigured）	风险	节点	错误

事件名称（陷阱名称）	影响级别	源类型	严重性
存储故障转移状态 - 接管（ocumEvtSfoStateTakeover）	风险	节点	警告
存储故障转移状态 - 部分交还（ocumEvtSfoStatePartialGiveback）	风险	节点	错误
存储故障转移节点状态为已关闭（ocumEvtSfoNodeStatusDown）	风险	节点	错误
无法执行存储故障转移接管（ocumEvtSfoTakeoverNotPossible）	风险	节点	错误

了解 **Active IQ Unified Manager** 中的存储服务事件

存储服务事件为您提供有关创建和订阅存储服务的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
存储服务已创建（不适用）	事件	存储服务	信息
已订阅存储服务（不适用）	事件	存储服务	信息
存储服务已取消订阅（不适用）	事件	存储服务	信息

影响区域：保护

事件名称（陷阱名称）	影响级别	源类型	严重性
意外删除受管 SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion	风险	存储服务	警告
意外删除存储服务成员卷（ocumEvtStorageServiceUnexpectedVolumeDeletion）	意外事件	存储服务	关键

了解 **Active IQ Unified Manager** 中的存储架事件

存储磁盘架事件会告诉您存储磁盘架是否出现异常，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重性。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
电压范围异常（ocumEvtShelfVoltageAbnormal）	风险	存储架	警告
异常电流范围（ocumEvtShelfCurrentAbnormal）	风险	存储架	警告
温度异常（ocumEvtShelfTemperatureAbnormal）	风险	存储架	警告

了解 **Active IQ Unified Manager** 中的 **Storage VM** 事件

存储 VM（存储虚拟机，也称为 SVM）事件可为您提供有关存储 VM（SVM）状态的信息，以便您可以监视潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
Storage VM CIFS 服务已关闭（ocumEvtVserverCifsServiceStatusDown）	意外事件	SVM	关键
SVM CIFS 服务未配置（不适用）	事件	SVM	信息
尝试连接不存在的 CIFS 共享*（nbladeCifsNoPrivShare）	意外事件	SVM	关键
CIFS NetBIOS 名称冲突 *（nbladeCifsNbNameConflict）	风险	SVM	错误
CIFS 卷影复制操作失败 *（cifsShadowCopyFailure）	风险	SVM	错误

事件名称（陷阱名称）	影响级别	源类型	严重性
许多 CIFS 连接 *（nbladeCifsManyAuths）	风险	SVM	错误
超出 CIFS 连接数上限 *（nbladeCifsMaxOpenSameFile）	风险	SVM	错误
超出每用户 CIFS 连接数上限 *（nbladeCifsMaxSessPerUsrConn）	风险	SVM	错误
SVM FC/FCoE 服务关闭（ocumEvtVserverFcServiceStatusDown）	意外事件	SVM	关键
SVM iSCSI 服务已关闭（ocumEvtVserverIscsiServiceStatusDown）	意外事件	SVM	关键
Storage VM NFS 服务已关闭（ocumEvtVserverNfsServiceStatusDown）	意外事件	SVM	关键
SVM FC/FCoE 服务未配置（不适用）	事件	SVM	信息
SVM iSCSI 服务未配置（不适用）	事件	SVM	信息
SVM NFS 服务未配置（不适用）	事件	SVM	信息
Storage VM 已停止（ocumEvtVserverDown）	风险	SVM	警告
AV 服务器太忙，无法接受新的扫描请求 *（nbladeVscanConnBackPressure）	风险	SVM	错误
没有可用于病毒扫描的 AV 服务器连接 *（nbladeVscanNoScannerConn）	意外事件	SVM	关键
未注册 AV 服务器 *（nbladeVscanNoRegdScanner）	风险	SVM	错误
AV 服务器连接无响应 *（nbladeVscanConnInactive）	事件	SVM	信息

事件名称（陷阱名称）	影响级别	源类型	严重性
未经授权的用户尝试访问 AV 服务器 *（nbladeVscanBadUserPrivAccess）	风险	SVM	错误
AV 服务器发现病毒 *（nbladeVscanVirusDetected）	风险	SVM	错误

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
已发现 SVM（不适用）	事件	SVM	信息
SVM 已删除（不适用）	事件	集群	信息
SVM 已重命名（不适用）	事件	SVM	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
SVM IOPS 严重阈值已违反（ocumSvmIopsIncident）	意外事件	SVM	关键
已违反 SVM IOPS 警告阈值（ocumSvmIopsWarning）	风险	SVM	警告
已违反 SVM MB/s 严重阈值（ocumSvmMbpsIncident）	意外事件	SVM	关键
已违反 SVM MB/s 警告阈值（ocumSvmMbpsWarning）	风险	SVM	警告
已违反 SVM 延迟严重阈值（ocumSvmLatencyIncident）	意外事件	SVM	关键
已违反 SVM 延迟警告阈值（ocumSvmLatencyWarning）	风险	SVM	警告

影响区域：安全性

事件名称（陷阱名称）	影响级别	源类型	严重性
审核日志已禁用（ocumVserverAuditLogDisabled）	风险	SVM	警告
登录横幅已禁用（ocumVserverLoginBannerDisabled）	风险	SVM	警告
SSH 正在使用不安全密码（ocumVserverSSHInsecure）	风险	SVM	警告
登录横幅已更改（ocumVserverLoginBannerChanged）	风险	SVM	警告
Storage VM 反勒索软件监控已禁用（antiRansomwareSvmStateDisabled）	风险	SVM	警告
Storage VM 反勒索软件监控已启用（学习模式）（antiRansomwareSvmStateDryrun）	事件	SVM	信息
适用于反勒索软件监控的 Storage VM（学习模式）（ocumEvtSvmArwCandidate）	事件	SVM	信息

了解 **Active IQ Unified Manager** 中的用户和组配额事件

用户和组配额事件为您提供有关用户和用户组配额容量以及文件和磁盘限制的信息，以便您可以监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、源类型和严重程度。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反用户或组配额磁盘空间软限制（ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached）	风险	用户或组配额	警告
已达到用户或组配额磁盘空间硬限制（ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached）	意外事件	用户或组配额	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反用户或组配额文件数软限制（ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached）	风险	用户或组配额	警告
已达到用户或组配额文件数硬限制（ocumEvtUserOrGroupQuotaFileCountHardLimitReached）	意外事件	用户或组配额	关键

了解 **Active IQ Unified Manager** 中的卷事件

卷事件提供有关卷状态的信息，使您能够监控潜在问题。事件按影响区域分组，包括事件名称、陷阱名称、影响级别、源类型和严重程度。

星号（*）用于标识已转换为 Unified Manager 事件的 EMS 事件。

影响区域：可用性

事件名称（陷阱名称）	影响级别	源类型	严重性
卷受限（ocumEvtVolumeRestricted）	风险	卷	警告
卷脱机（ocumEvtVolumeOffline）	意外事件	卷	关键
卷部分可用（ocumEvtVolumePartiallyAvailable）	风险	卷	错误
卷已卸载（不适用）	事件	卷	信息
卷已挂载（不适用）	事件	卷	信息
卷已重新挂载（不适用）	事件	卷	信息
卷接合路径非活动（ocumEvtVolumeJunctionPathInactive）	风险	卷	警告
已启用卷自动调整大小（不适用）	事件	卷	信息
卷自动调整大小-禁用（不适用）	事件	卷	信息
卷自动调整大小最大容量已修改（不适用）	事件	卷	信息
卷自动调整大小增量大小已修改（不适用）	事件	卷	信息

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
精简配置卷空间存在风险（ocumThinProvisionVolumeSpaceAtRisk）	风险	卷	警告
卷效率操作错误（ocumEvtVolumeEfficiencyOperationError）	风险	卷	错误
卷空间已满（ocumEvtVolumeFull）	风险	卷	错误
卷空间接近全满（ocumEvtVolumeNearlyFull）	风险	卷	警告
卷逻辑空间已满 *（volumeLogicalSpaceFull）	风险	卷	错误
卷逻辑空间接近全满 *（volumeLogicalSpaceNearlyFull）	风险	卷	警告
卷逻辑空间正常 *(volumeLogicalSpaceAllOK)	事件	卷	信息
卷 Snapshot 预留空间已满（ocumEvtSnapshotFull）	风险	卷	警告
Snapshot 副本太多（ocumEvtSnapshotTooMany）	风险	卷	错误
卷 Qtree 配额已过量提交（ocumEvtVolumeQtreeQuotaOvercommitted）	风险	卷	错误
卷 Qtree 配额接近过量提交（ocumEvtVolumeQtreeQuotaAlmostOvercommitted）	风险	卷	警告
卷增长率异常（ocumEvtVolumeGrowthRateAbnormal）	风险	卷	警告
卷达到全满前的天数（ocumEvtVolumeDaysUntilFullSoon）	风险	卷	错误
卷空间保证已禁用（不适用）	事件	卷	信息

事件名称（陷阱名称）	影响级别	源类型	严重性
卷空间保证已启用（不适用）	事件	卷	信息
卷空间保证已修改（不适用）	事件	卷	信息
卷 Snapshot 预留达到全满前的天数（ocumEvtVolumeSnapshotReserveDaysUntilFullSoon）	风险	卷	错误
FlexGroup 成分存在空间问题 *（flexGroupConstituentsHaveSpaceIssues）	风险	卷	错误
FlexGroup 成分卷空间状态一切正常 *(flexGroupConstituentsSpaceStatusAllOK)	事件	卷	信息
FlexGroup 成分卷存在索引节点问题*（flexGroupConstituentsHaveInodesIssues）	风险	卷	错误
FlexGroup 成分卷 Inode 状态全部正常 *(flexGroupConstituentsInodesStatusAllOK)	事件	卷	信息
WAFL 卷 AutoSize 失败 *（waflVolAutoSizeFail）	风险	卷	错误
WAFL 卷 AutoSize 已完成*（waflVolAutoSizeDone）	事件	卷	信息
FlexGroup 卷利用率超过 80%*	意外事件	卷	错误
FlexGroup 卷利用率超过 90%*	意外事件	卷	关键
卷存储效率异常（ocumVolumeAbnormalStorageEfficiencyWarning）	风险	卷	警告
卷 Snapshot 预留未充分利用（volumeSnaphotReserveUnderutilizedWarning）	事件	卷	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
卷 Snapshot 预留未充分利用（volumeSnaphotReserveUnderutilizedCleared）	事件	卷	警告

影响区域：配置

事件名称（陷阱名称）	影响级别	源类型	严重性
卷已重命名（不适用）	事件	卷	信息
发现的卷（不适用）	事件	卷	信息
卷已删除（不适用）	事件	卷	信息

影响区域：性能

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反 QoS 卷最大 IOPS 警告阈值（ocumQosVolumeMaxIopsWarning）	风险	卷	警告
已违反 QoS 卷最大 MB/s 警告阈值（ocumQosVolumeMaxMbpsWarning）	风险	卷	警告
已违反 QoS 卷最大 IOPS/TB 警告阈值（ocumQosVolumeMaxIopsPerTbWarning）	风险	卷	警告
已违反性能服务级别策略定义的工作负载卷延迟阈值（ocumConformanceLatencyWarning）	风险	卷	警告
已违反卷 IOPS 严重阈值（ocumVolumeIopsIncident）	意外事件	卷	关键
已违反卷 IOPS 警告阈值（ocumVolumeIopsWarning）	风险	卷	警告
已违反卷 MB/s 严重阈值（ocumVolumeMbpsIncident）	意外事件	卷	关键
卷 MB/s 警告阈值已突破（ocumVolumeMbpsWarning ）	风险	卷	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反卷延迟严重阈值（ocumVolumeLatencyIncident）	意外事件	卷	关键
已违反卷延迟警告阈值（ocumVolumeLatencyWarning）	风险	卷	警告
已违反卷缓存未命中率严重阈值（ocumVolumeCacheMissRatioIncident）	意外事件	卷	关键
已违反卷缓存未命中率警告阈值（ocumVolumeCacheMissRatioWarning）	风险	卷	警告
已违反卷延迟和 IOPS 严重阈值（ocumVolumeLatencyIopsIncident）	意外事件	卷	关键
已违反卷延迟和 IOPS 警告阈值（ocumVolumeLatencyIopsWarning）	风险	卷	警告
已违反卷延迟和 MB/s 严重阈值（ocumVolumeLatencyMbpsIncident）	意外事件	卷	关键
已违反卷延迟和 MB/s 警告阈值（ocumVolumeLatencyMbpsWarning）	风险	卷	警告
已违反卷延迟和聚合已用性能容量严重阈值（ocumVolumeLatencyAggregatePerfCapacityUsedIncident）	意外事件	卷	关键
已违反卷延迟和聚合已用性能容量警告阈值（ocumVolumeLatencyAggregatePerfCapacityUsedWarning）	风险	卷	警告
已违反卷延迟和聚合利用率严重阈值（ocumVolumeLatencyAggregateUtilizationIncident）	意外事件	卷	关键

事件名称（陷阱名称）	影响级别	源类型	严重性
已违反卷延迟和聚合利用率警告阈值（ocumVolumeLatencyAggregateUtilizationWarning）	风险	卷	警告
已违反卷延迟和节点已用性能容量严重阈值（ocumVolumeLatencyNodePerfCapacityUsedIncident）	意外事件	卷	关键
已违反卷延迟和节点已用性能容量警告阈值（ocumVolumeLatencyNodePerfCapacityUsedWarning）	风险	卷	警告
卷延迟和已用节点性能容量 - 已违反接管严重阈值（ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident）	意外事件	卷	关键
卷延迟和已用节点性能容量 - 已违反接管警告阈值（ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning）	风险	卷	警告
已违反卷延迟和节点利用率严重阈值（ocumVolumeLatencyNodeUtilizationIncident）	意外事件	卷	关键
已违反卷延迟和节点利用率警告阈值（ocumVolumeLatencyNodeUtilizationWarning）	风险	卷	警告

影响区域：安全性

事件名称（陷阱名称）	影响级别	源类型	严重性
卷反勒索软件监控已启用（活动模式）（antiRansomwareVolumeStateEnabled）	事件	卷	信息
卷反勒索软件监控已禁用（antiRansomwareVolumeStateDisabled）	风险	卷	警告

事件名称（陷阱名称）	影响级别	源类型	严重性
卷反勒索软件监控已启用（学习模式）（antiRansomwareVolumeStateDryrun）	事件	卷	信息
卷反勒索软件监控已暂停（学习模式）（antiRansomwareVolumeStateDryrunPaused）	风险	卷	警告
卷反勒索软件监控已暂停（活动模式）（antiRansomwareVolumeStateEnablePaused）	风险	卷	警告
卷防勒索软件监控正在禁用（antiRansomwareVolumeStateDisableInProgress）	风险	卷	警告
已发现勒索软件活动（callHomeRansomwareActivitySeen）	意外事件	卷	关键
适用于反勒索软件监控的卷（学习模式）（ocumEvtVolumeArwCandidate）	事件	卷	信息
适用于反勒索软件监控的卷（活动模式）（ocumVolumeSuitedForActiveAntiRansomwareDetection）	风险	卷	警告
卷显示频繁的反勒索软件警报（antiRansomwareFeatureNoisyVolume）	风险	卷	警告

影响领域：数据保护

事件名称（陷阱名称）	影响级别	源类型	严重性
卷的本地快照保护不足（volumeLacksLocalProtectionWarning）	风险	卷	警告
卷的本地快照保护不足（volumeLacksLocalProtectionCleared）	风险	卷	警告

了解 **Active IQ Unified Manager** 中的卷移动状态事件

卷移动状态事件可告知您卷移动的状态，以便您监控潜在问题。事件按影响区域分组，包括事件和陷阱名称、影响级别、来源类型和严重程度。

影响区域：容量

事件名称（陷阱名称）	影响级别	源类型	严重性
卷移动状态：正在进行中（不适用）	事件	卷	信息
卷移动状态 - 失败（ocumEvtVolumeMoveFailed）	风险	卷	错误
卷移动状态：已完成（不适用）	事件	卷	信息
卷移动 - 转换延迟（ocumEvtVolumeMoveCutoverDeferred）	风险	卷	警告

事件窗口和对话框说明

了解 **Active IQ Unified Manager** 中的通知页面

您可以将 Unified Manager 服务器配置为在生成事件或将事件分配给用户时发送通知。您还可以配置通知机制。例如，通知可以作为电子邮件或 SNMP 陷阱发送。

您必须具有应用程序管理员或存储管理员角色。

电子邮件

此区域用于配置以下用于告警通知的电子邮件设置：

- 发件人地址

  指定发送警报通知的电子邮件地址。此值在共享时也用作报告的发件人地址。如果发件人地址预先填写了地址“ActiveIQUnifiedManager@localhost.com”，则应将其更改为真实有效的电子邮件地址，以确保成功发送所有电子邮件通知。

SMTP 服务器

此区域用于配置以下 SMTP 服务器设置：

- 主机名或 **IP** 地址

  指定 SMTP 主机服务器的主机名，该主机名用于向指定的收件人发送警报通知。

- 用户名

  指定 SMTP 用户名。只有在 SMTP 服务器中启用 SMTPAUTH 时，才需要 SMTP 用户名。

- 密码

  指定 SMTP 密码。只有在 SMTP 服务器中启用 SMTPAUTH 时，才需要 SMTP 用户名。

- 端口

  指定 SMTP 主机服务器用于发送警报通知的端口。

  默认值为 25。

- 使用 **START/TLS**

  选中此框可通过使用 TLS/SSL 协议（也称为 start_tls 和 StartTLS）在 SMTP 服务器与管理服务器之间提供安全通信。

- 使用 **SSL**

  选中此框可使用 SSL 协议在 SMTP 服务器和管理服务器之间提供安全通信。

SNMP

此区域用于配置以下 SNMP 陷阱设置：

- 版本

  根据所需的安全类型指定要使用的 SNMP 版本。选项包括版本 1、版本 3、版本 3（含身份验证）和版本 3（含身份验证和加密）。默认值为版本 1。

- **Trap** 目标主机

  指定接收管理服务器发送的 SNMP 陷阱的主机名或 IP 地址（IPv4 或 IPv6）。要指定多个陷阱目的地，请使用逗号分隔每个主机。

  所有其他 SNMP 设置（例如“版本”和“出站端口”）对于此列表中的所有主机必须相同。

- 出站陷阱端口

  指定 SNMP 服务器接收管理服务器发送的陷阱所通过的端口。

  默认值为 162。

- 社区

  用于访问主机的社区字符串。

- 引擎 **ID**

  指定 SNMP 代理的唯一标识符，并由管理服务器自动生成。引擎 ID 可用于 SNMP 版本 3、SNMP 版本 3（含身份验证）和 SNMP 版本 3 （含身份验证和加密）。

- 用户名

指定 SNMP 用户名。用户名可用于 SNMP 版本 3、SNMP 版本 3（含身份验证）和 SNMP 版本 3（含身份验证和加密）。

- 身份验证协议

  指定用于对用户进行身份验证的协议。协议选项包括 MD5 和 SHA。MD5 是默认值。身份验证协议可用于 SNMP 版本 3 （含身份验证）和 SNMP 版本 3 （含身份验证和加密）。

- 身份验证密码

  指定对用户进行身份验证时使用的密码。SNMP 版本 3（含身份验证）和 SNMP 版本 3（含身份验证和加密）提供身份验证密码。

- 隐私协议

  指定用于加密 SNMP 消息的隐私协议。协议选项包括 AES 128 和 DES。默认值为 AES 128。隐私协议适用于具有身份验证和加密功能的 SNMP 版本 3。

- 隐私密码

  指定使用隐私协议时的密码。隐私密码可用于具有身份验证和加密的 SNMP 版本 3。

有关 SNMP 对象和陷阱的详细信息，您可以从 NetApp 支持站点下载 "Active IQ Unified Manager MIB"。

了解 **Active IQ Unified Manager** 中的事件管理清单页面

事件管理清单页面使您能够查看当前事件及其属性的列表。您可以执行确认、解决和分配事件等任务。您还可以为特定事件添加警报。

此页面上的信息每 5 分钟自动刷新一次，以确保显示最新的新事件。

筛选组件

使您能够自定义事件列表中显示的信息。可以使用以下组件优化显示的事件列表：

- 查看菜单可从预定义的筛选器选择列表中进行选择。

  这包括所有活动（新建和确认）事件、活动性能事件、分配给我（登录用户）的事件以及所有维护期间生成的所有事件等项目。

- 搜索窗格，用于通过输入完整或部分术语来细化事件列表。
- 用于启动“筛选器”窗格的“筛选器”按钮，以便您可以从每个可用的字段和字段属性中进行选择以优化事件列表。

命令按钮

这些命令按钮可用来执行下列任务：

- 分配给

  使您能够选择要将事件分配给的用户。将事件分配给用户时，用户名和分配事件的时间将添加到所选事件的事件列表中。

- 自己

  将事件分配给当前登录的用户。

- 其他用户

  显示“分配所有者”对话框，通过该对话框可以将事件分配或重新分配给其他用户。您也可以将所有权字段留空以取消分配事件。

- 确认

  确认选定事件。

  当您确认事件时，您的用户名和确认事件的时间将添加到选定事件的事件列表中。当您确认某个事件时，您有责任管理该事件。

  您无法确认信息事件。

- 标记为已解决

  使您能够将事件状态更改为已解决。

  解决事件时，您的用户名和解决该事件的时间将添加到所选事件的事件列表中。对事件采取纠正措施后，必须将该事件标记为已解决。

- 添加警报

  显示“添加警报”对话框，用于为选定事件添加警报。

- 报告

  使您能够将当前事件视图的详细信息导出为逗号分隔值 (.csv) 文件或 PDF 文档。

- 显示/隐藏列选择器

  使您能够选择在页面上显示的列，并选择它们的显示顺序。

事件列表

显示按触发时间排序的所有事件的详细信息。

默认情况下，将显示所有活动事件视图，以显示前七天具有事件或风险影响级别的新事件和已确认事件。

- 触发时间

  生成事件的时间。

- 严重程度

  事件严重性：Critical （严重） （）、Error （错误） （）、Warning （警告） （）和 Information （信息） （）。

- **State**

  事件状态：新建、已确认、已解决或已废弃。

- 影响级别

  事件影响级别：突发事件、风险、事件或升级。

- 影响区域

  事件影响区域：可用性、容量、性能、保护、配置或安全性。

- 名称

  事件名称。您可以选择名称以显示该事件的“事件详细信息”页面。

- 源

  已发生事件的对象名称。您可以选择名称以显示该对象的运行状况或性能详细信息页面。

  当发生共享 QoS 策略违规时，此字段中仅显示占用最多 IOPS 或 MB/s 的工作负载对象。使用此策略的其他工作负载将显示在事件详细信息页面中。

- 源类型

  与事件关联的对象类型（例如，Storage VM、卷或 Qtree）。

- 分配给

  事件分配到的用户名称。

- 事件起源

  事件是源自“Active IQ Portal”还是直接源自“Active IQ Unified Manager”。

- 注释名称

  分配给存储对象的批注的名称。

- 备注

  为事件添加的注释数。

- 待处理天数

  事件最初生成后的天数。

- 分配时间

  事件分配给用户后经过的时间。如果经过的时间超过一周，则会显示事件分配给用户的时间戳。

- 确认人

确认此事件的用户的名称。如果事件未确认，此字段为空。

- 确认时间

  事件确认后经过的时间。如果经过的时间超过一周，则会显示事件确认的时间戳。

- 解决者

  解决事件的用户的名称。如果事件未解决，则此字段为空。

- 解决时间

  事件解决后经过的时间。如果经过的时间超过一周，则会显示事件解决的时间戳。

- 废弃时间

  事件状态变为已过时的时间。

事件详细信息页面

了解 **Active IQ Unified Manager** 中的事件详细信息页面

从“事件详细信息”页面，您可以查看所选事件的详细信息，例如事件严重程度、影响级别、影响区域和事件源。您还可以查看有关可能的修复措施的其他信息，以解决此问题。

- 事件名称

  事件的名称和上次发现事件的时间。

  对于非性能事件，当事件处于“新建”或“已确认”状态时，最后看到的信息未知，因此被隐藏。

- 事件描述

  对事件的简要描述。

  在某些情况下，事件触发的原因会在事件描述中提供。

- 争用组件

  对于动态性能事件，此部分显示表示集群的逻辑和物理组件的图标。如果组件处于争用状态，其图标将带圆圈并突出显示为红色。

  有关此处显示的组件的说明，请参阅 *Cluster components and why they can be in contention*。

事件信息、系统诊断和建议操作部分在其他主题中进行了说明。

命令按钮

这些命令按钮可用来执行下列任务：

- 备注图标

使您可以添加或更新有关事件的备注，并查看其他用户留下的所有备注。

操作菜单

- 分配给我

  将此事件分配给您。

- 分配给其他人

  打开“分配所有者”对话框，用于将事件分配或重新分配给其他用户。

  将事件分配给用户时，用户的名称和事件分配的时间将添加到选定事件的事件列表中。

  您也可以将所有权字段留空，以取消分配事件。

- 确认

  确认所选事件，这样您就不会继续收到重复警报通知。

  当您确认事件时，您的用户名和确认事件的时间将添加到选定事件的事件列表（确认人）中。当您确认某个事件时，您负责管理该事件。

- 标记为已解决

  使您能够将事件状态更改为“已解决”。

  当您解决事件时，您的用户名和解决该事件的时间将添加到所选事件的事件列表（解决者）中。对事件采取纠正措施后，必须将该事件标记为已解决。

- 添加警报

  显示“添加警报”对话框，用于为选定事件添加警报。

了解 **Active IQ Unified Manager** 中的事件信息部分

您可以使用事件详细信息页面上的"事件信息"部分，查看有关所选事件的详细信息，例如事件严重性、影响级别、影响区域和事件源。

不适用于该事件类型的字段将被隐藏。您可以查看以下事件详细信息：

- 事件触发时间

  生成事件的时间。

- **State**

  事件状态：新建、已确认、已解决或已废弃。

- 废弃原因

  导致事件被废弃的操作，例如，问题已修复。

- 事件持续时间

  对于活动（新建和已确认）事件，这是检测到事件与上次分析事件之间的时间。对于过时的事件，这是检测到事件和解决事件之间的时间。

  此字段针对所有性能事件显示，对于其他事件类型，仅在它们已解决或已过时后才显示。

- 上次查看时间

  上次将事件显示为活动的日期和时间。

  对于性能事件，此值可能比事件触发时间更新，因为只要事件处于活动状态，此字段就会在每次新的性能数据收集之后更新。对于其他类型的事件，当处于“新建”或“已确认”状态时，此内容不会更新，因此该字段将被隐藏。

- 严重程度

  事件严重性：Critical （严重） （）、Error （错误） （）、Warning （警告） （）和 Information （信息） （）。

- 影响级别

  事件影响级别：突发事件、风险、事件或升级。

- 影响区域

  事件影响区域：可用性、容量、性能、保护、配置或安全性。

- 源

  发生事件的对象的名称。

  查看共享 QoS 策略事件的详细信息时，此字段中最多会列出三个消耗 IOPS 或 MBps 最多的工作负载对象。

  您可以单击源名称链接来显示该对象的运行状况或性能详细信息页面。

- 源注释

  显示与事件关联的对象的批注名称和值。

  此字段仅对群集、SVM 和卷上的运行状况事件显示。

- 源组

  显示受影响对象所属的所有组的名称。

  此字段仅对群集、SVM 和卷上的运行状况事件显示。

- 源类型

  与事件关联的对象类型（例如 SVM、Volume 或 Qtree）。

- 在集群上

  发生事件的集群的名称。

  您可以单击集群名称链接来显示该集群的运行状况或性能详细信息页面。

- 受影响对象计数

  受此事件影响的对象数。

  您可以单击对象链接来显示包含当前受此事件影响的对象的清单页面。

  此字段仅针对性能事件显示。

- 受影响的卷

  受此事件影响的卷数。

  此字段仅针对节点或聚合上的性能事件显示。

- 触发策略

  发出事件的阈值策略的名称。

  您可以将光标悬停在策略名称上，以查看阈值策略的详细信息。对于自适应 QoS 策略，还会显示定义的策略、块大小和分配类型（分配空间或已用空间）。

  此字段仅针对性能事件显示。

- 规则 **ID**

  对于 Active IQ 平台事件，这是触发生成此事件的规则编号。

- 确认人

  确认该事件的人员的姓名和确认该事件的时间。

- 解决者

  解决事件的人员姓名和事件解决的时间。

- 分配给

  被指派处理该事件的人员的姓名。

- 警报设置

  此时将显示有关警报的以下信息：

  - 如果没有与选定事件关联的警报，则会显示*添加警报*链接。

    您可以通过单击链接打开“添加警报”对话框。

- 如果有一个警报与所选事件关联，则会显示警报名称。

  您可以通过单击链接打开“编辑警报”对话框。

- 如果有多个警报与所选事件相关联，则会显示警报数量。

  您可以通过单击链接打开“警报设置”页面，以查看有关这些警报的更多详细信息。

已禁用的警报不会显示。

- 上次发送的通知

  发送最新警报通知的日期和时间。

- 发送方式

  用于发送警报通知的机制：电子邮件或 SNMP 陷阱。

- 上次脚本运行

  生成警报时所执行脚本的名称。

了解 **Active IQ Unified Manager** 中的建议操作

“事件详细信息”页面的“建议操作”部分提供了此事件的可能原因，并建议了一些操作，以便您可以尝试自行解决此事件。建议的操作是根据已违反的事件类型或阈值类型进行自定义的。

此区域仅针对某些类型的事件显示。

在某些情况下，页面上提供的*帮助*链接会引用许多建议操作的其他信息，包括执行特定操作的说明。其中一些操作可能涉及使用 Unified Manager、ONTAP System Manager、OnCommand Workflow Automation、ONTAP CLI 命令或这些工具的组合。

此处建议的操作仅供解决事件时参考。您应根据具体环境情况来确定用于解决此事件的操作。

如果要更详细地分析对象和事件，请单击*分析工作负载*按钮以显示工作负载分析页面。

Unified Manager 可以彻底诊断某些事件并提供单一解决方案。如果可用，这些解决方案将通过 修复 按钮显示。单击此按钮可让 Unified Manager 修复导致此事件的问题。

对于 Active IQ 平台事件，此部分可能包含指向 NetApp 知识库文章的链接（如果可用），该文章描述了问题和可能的解决方案。在没有外部网络访问权限的站点中，知识库文章的 PDF 将在本地打开；该 PDF 是手动下载到 Unified Manager 实例的规则文件的一部分。

了解 **Active IQ Unified Manager** 中的系统诊断

“事件详细信息”页面的“系统诊断”部分提供了可以帮助您诊断可能导致该事件的问题的信息。

此区域仅针对某些事件显示。

某些性能事件会提供与已触发的特定事件相关的图表。通常，这包括前十天的 IOPS 或 MBps 图表以及延迟图表。以这种方式排列后，您可以看到在事件处于活动状态时，哪些存储组件对延迟的影响最大，或受延迟影响最大。

对于动态性能事件，将显示以下图表：

- 工作负载延迟 - 显示处于争用状态的组件中最严重的受害者、欺凌者或鲨鱼工作负载的延迟历史记录。
- 工作负载活动 - 显示有关处于争用状态的集群组件的工作负载使用情况的详细信息。
- 资源活动 - 显示争用中的集群组件的历史性能统计信息。

当某些集群组件处于争用状态时，将显示其他图表。

其他事件提供了系统对存储对象执行的分析类型的简要描述。在某些情况下，会有一行或多行；对于分析多个性能计数器的系统定义性能策略，每个已分析的组件对应一行。在这种情况下，诊断旁边将显示一个绿色或红色图标，以指示在该特定诊断中是否发现了问题。

了解 **Active IQ Unified Manager** 中的事件设置页面

"Event Setup"页面显示已禁用的事件列表，并提供关联对象类型和事件严重性等信息。您也可以执行全局禁用或启用事件等任务。

仅当您具有应用程序管理员或存储管理员角色时，才能访问此页面。

命令按钮

命令按钮可用于为所选事件执行以下任务：

- 禁用

  启动“禁用事件”对话框，您可以使用它来禁用事件。

- 启用

  启用之前选择禁用的选定事件。

- 上传规则

  启动“上传规则”对话框，使没有外部网络访问权限的站点能够手动将 Active IQ 规则文件上传到 Unified Manager。这些规则根据群集 AutoSupport 消息运行，以生成 Active IQ 平台定义的系统配置、布线、最佳实践和可用性的事件。

- 订阅 **EMS** 事件

  启动 Subscribe to EMS Events（订阅 EMS 事件）对话框，使您能够订阅从正在监视的集群接收特定事件管理系统 (EMS) 事件。EMS 收集有关集群上发生的事件的信息。当收到已订阅 EMS 事件的通知时，将生成具有适当严重程度的 Unified Manager 事件。

列表视图

列表视图以表格格式显示有关已禁用事件的信息。您可以使用列筛选器自定义显示的数据。

- 事件

  显示已禁用事件的名称。

- 严重程度

  显示事件的严重程度。严重程度可以是严重、错误、警告或信息。

- 源类型

  显示为其生成事件的源类型。

禁用 **Active IQ Unified Manager** 中的**"**事件**"**对话框

“禁用事件”对话框显示可以禁用事件的事件类型列表。您可以根据特定严重程度或针对一组事件禁用事件类型的事件。

您必须具有应用程序管理员或存储管理员角色。

事件属性区域

事件属性区域指定以下事件属性：

- 事件严重程度

  使您能够根据严重程度类型选择事件，严重程度类型可以是“严重”、“错误”、“警告”或“信息”。

- 事件名称包含

  使您能够筛选名称包含指定字符的事件。

- 匹配事件

  显示与事件严重性类型和您指定的文本字符串匹配的事件列表。

- 禁用事件

  显示选定要禁用的事件列表。

  还会显示事件的严重性以及事件名称。

命令按钮

通过命令按钮，可以为选定事件执行以下任务：

- 保存并关闭

  禁用此事件类型并关闭此对话框。

- 取消

  放弃更改并关闭对话框。

管理提醒

了解 **Active IQ Unified Manager** 中的警报

虽然事件不断发生，但 Unified Manager 仅在事件满足指定的过滤条件时才会生成警报。您可以选择应为其生成警报的事件，例如，当超过空间阈值或对象脱机时。您还可以将警报与触发警报时执行的脚本相关联。

筛选条件包括对象类、名称或事件严重性。

Active IQ Unified Manager 警报电子邮件中包含的信息

Unified Manager 警报电子邮件提供事件的类型、事件的严重性、被违反并导致事件的策略或阈值的名称以及事件的描述。电子邮件消息还为每个事件提供了一个超链接，使您能够在 UI 中查看该事件的详细信息页面。

警报电子邮件将发送给已订阅接收警报的所有用户。

如果性能计数器或容量值在收集期间发生较大变化，则可能会导致同一阈值策略同时触发严重事件和警告事件。在这种情况下，您可能会收到一封关于警告事件的电子邮件和一封关于严重事件的电子邮件。这是因为 Unified Manager 允许您单独订阅以接收警告和严重阈值违规的警报。

警报电子邮件示例如下所示：

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

A risk was generated by 10.11.12.13 that requires your attention.

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

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

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

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

添加警报

在 **Active IQ Unified Manager** 中添加警报

您可以配置警报，以便在生成特定事件时通知您。可以为单个资源、一组资源或特定严重性类型的事件配置警报。您可以指定要收到通知的频率，并将脚本关联到警报。

开始之前

- 您必须配置通知设置（如用户电子邮件地址、SMTP 服务器和 SNMP 陷阱主机），以使 Active IQ Unified Manager 服务器能够在生成事件时使用这些设置向用户发送通知。
- 您必须知道要触发警报的资源和事件，以及要通知的用户的用户名或电子邮件地址。
- 如果要根据事件执行脚本，则必须使用“脚本”页面将脚本添加到 Unified Manager。
- 您必须具有应用程序管理员或存储管理员角色。

除了从“警报设置”页面创建警报之外，您还可以在收到事件后直接从“事件详细信息”页面创建警报，如此处所述。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。
2. 在*警报设置*页面中，单击*添加*。
3. 在*添加警报*对话框中，单击*名称*，并输入警报的名称和描述。
4. 单击*资源*，然后选择要包含在此警报中或从此警报中排除的资源。

   您可以通过在*名称包含*字段中指定文本字符串来设置筛选器，以选择一组资源。根据指定的文本字符串，可用资源列表仅显示与筛选规则匹配的资源。指定的文本字符串区分大小写。

   如果资源同时符合已指定的包含和排除规则，则排除规则优先于包含规则，并且不会为与排除资源相关的事件生成警报。

5. 单击*事件*，并根据要触发警报的事件名称或事件严重性类型选择事件。

   要选择多个事件，请在进行选择时按 Ctrl 键。

6. 单击 操作，选择要通知的用户，选择通知频率，选择是否将 SNMP 陷阱发送到陷阱接收器，并分配生成警报时要执行的脚本。

   如果修改为用户指定的电子邮件地址并重新打开警报进行编辑，则“名称”字段将显示为空白，因为修改后的电子邮件地址不再映射到先前选择的用户。此外，如果从“用户”页面修改了所选用户的电子邮件地址，则不会为所选用户更新已修改的电子邮件地址。

   您也可以选择通过 SNMP 陷阱通知用户。

7. 单击 **Save**。

添加警报的示例

此示例演示如何创建满足以下要求的警报：

- 警报名称：HealthTest
- 资源：包括名称包含“abc”的所有卷，不包括名称包含“xyz”的所有卷
- 事件：包括所有严重运行状况事件
- 操作：包括“sample@domain.com”、“Test”脚本，并且必须每 15 分钟通知一次用户

请在添加警报对话框中执行以下步骤：

1. 单击*名称*，然后在*警报名称*字段中输入 **`HealthTest`**。
2. 单击*资源*，然后在包含选项卡中，从下拉列表中选择*卷*。
   a. 在*名称包含*字段中输入 **`abc`**，以显示名称包含 "abc" 的卷。
   b. 从可用资源区域中选择 **<<All Volumes whose name contains 'abc'>>**，并将其移动到选定资源区域。
   c. 单击 排除，在 名称包含 字段中输入 **`xyz`**，然后单击 添加。
3. 单击*事件*，然后从事件严重性字段中选择*严重*。
4. 从"匹配事件"区域中选择 **All Critical Events**，然后将其移动到"已选择事件"区域。
5. 单击*操作*，然后在提醒这些用户字段中输入*`sample@domain.com`*。
6. 选择*每 15 分钟提醒一次*，每 15 分钟通知一次用户。

   您可以将警报配置为在指定时间内重复向收件人发送通知。您应确定警报的事件通知处于活动状态的时间。
7. 在“Select Script to Execute”菜单中，选择 **Test** 脚本。
8. 单击 **Save**。

在 **Active IQ Unified Manager** 中添加警报的准则

您可以根据资源（如群集、节点、聚合或卷）以及特定严重性类型的事件添加警报。作为最佳做法，您可以在添加对象所属的群集后，为任何关键对象添加警报。

您可以使用以下指南和注意事项来创建警报，以有效地管理您的系统：

- 警报说明

  您应提供警报的描述，以帮助您有效跟踪警报。

- 资源

  您应该决定哪个物理或逻辑资源需要警报。您可以根据需要包括和排除资源。例如，如果要通过配置警报来密切监视聚合，则必须从资源列表中选择所需的聚合。

  如果您选择一个资源类别，例如 **<<All User or Group Quotas>>**，则您将收到该类别中所有对象的警报。

  > 选择集群作为资源不会自动选择该集群中的存储对象。例如，如果您为所有集群的所有严重事件创建警报，则只会收到集群严重事件的警报。您不会收到有关节点、聚合等严重事件的警报。

- 事件严重性

您应该决定指定严重程度类型（严重、错误、警告）的事件是否应触发警报，如果是，则决定哪种严重程度类型。

- 选定事件

  如果根据生成的事件类型添加警报，则应决定哪些事件需要警报。

  如果您选择事件严重程度，但未选择任何单个事件（如果将“所选事件”列留空），则您将收到该类别中所有事件的警报。

- 操作

  您必须提供接收通知的用户的用户名和电子邮件地址。您还可以将 SNMP 陷阱指定为通知模式。您可以将脚本与警报相关联，以便在生成警报时执行。

- 通知频率

  您可以将警报配置为在指定时间内重复向收件人发送通知。您应该确定警报的事件通知处于活动状态的时间。如果要在事件被确认之前重复事件通知，则应确定重复通知的频率。

- 执行脚本

  您可以将脚本与警报相关联。生成警报时会执行脚本。

在 **Active IQ Unified Manager** 中添加性能事件警报

您可以为单个性能事件配置警报，就像 Unified Manager 接收的任何其他事件一样。此外，如果您希望以相同方式处理所有性能事件，并将电子邮件发送给同一个人，则可以创建一个警报，以便在触发任何严重或警告性能事件时通知您。

开始之前

您必须具有应用程序管理员或存储管理员角色。

下面的示例演示如何为所有严重延迟、IOPS 和 MBps 事件创建事件。您可以使用相同的方法从所有性能计数器和所有警告事件中选择事件。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。
2. 在*警报设置*页面中，单击*添加*。
3. 在*添加警报*对话框中，单击*名称*，并输入警报的名称和描述。
4. 请勿在*资源*页面上选择任何资源。

   由于未选择任何资源，警报将应用于接收这些事件的所有集群、聚合、卷等。

5. 单击 事件 并执行以下操作：
   a. 在事件严重程度列表中，选择*严重*。
   b. 在事件名称包含字段中，输入*`latency`*，然后单击箭头以选择所有匹配的事件。
   c. 在事件名称包含字段中，输入 **`iops`**，然后单击箭头以选择所有匹配的事件。

d. 在事件名称包含字段中，输入 **mbps**，然后单击箭头以选择所有匹配的事件。

6. 单击*操作*，然后在*提醒这些用户*字段中选择将接收警报电子邮件的用户的名称。
7. 配置此页面上用于发出 SNMP 陷阱和执行脚本的任何其他选项。
8. 单击 **Save**。

在 **Active IQ Unified Manager** 中测试警报

您可以测试警报以验证其配置是否正确。触发事件时，将生成警报，并向配置的收件人发送警报电子邮件。您可以使用测试警报来验证通知是否已发送以及脚本是否已执行。

开始之前

- 您必须已配置通知设置，例如收件人的电子邮件地址、SMTP 服务器和 SNMP 陷阱。

  Unified Manager 服务器可以使用这些设置在生成事件时向用户发送通知。

- 您必须已分配脚本并将脚本配置为在生成警报时运行。
- 您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。
2. 在*警报设置*页面中，选择要测试的警报，然后单击*测试*。

   测试警报电子邮件将发送到您在创建警报时指定的电子邮件地址。

在 **Active IQ Unified Manager** 中禁用已解决和已过时事件的警报

对于已配置为发送警报的所有事件，当这些事件通过所有可用状态（新建、已解决和已过时）转换时，将发送警报消息。如果不希望在事件进入"已解决"和"已过时"状态时接收事件警报，则可以配置全局设置以抑制这些警报。

开始之前

您必须具有应用程序管理员或存储管理员角色。

默认情况下，事件进入“已解决”和“已废弃”状态时不会发送警报。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。
2. 在*警报设置*页面中，使用项目*已解决和已废弃事件的警报*旁边的滑块控件执行以下操作之一：

目的	操作
在事件已解决或已过时时停止发送警报	将滑块控件向左移动
在事件已解决或已过时时开始发送警报	将滑块控件向右移动

在 **Active IQ Unified Manager** 中排除灾难恢复目标卷以避免生成警报

配置卷警报时，您可以在“警报”对话框中指定一个字符串来标识一个卷或一组卷。但是，如果您已为 SVM 配置了灾难恢复，则源卷和目标卷具有相同的名称，因此您将收到两个卷的警报。

开始之前

您必须具有应用程序管理员或存储管理员角色。

可以通过排除具有目标 SVM 名称的卷来禁用灾难恢复目标卷的警报。这是可行的，因为卷事件的标识符同时包含 SVM 名称和卷名称，格式为“<svm_name>:/<volume_name>”。

以下示例显示如何在主 SVM “vs1” 上为卷 “vol1” 创建警报，但排除在 SVM “vs1-dr” 上的同名卷上生成警报。

请在添加警报对话框中执行以下步骤：

步骤

1. 单击*名称*并输入警报的名称和描述。
2. 单击*资源*，然后选择*包括*选项卡。
   a. 从下拉列表中选择*卷*，然后在*名称包含*字段中输入 **`vol1`**，以显示名称包含 "vol1" 的卷。
   b. 从*可用资源*区域选择 **<<All Volumes whose name contains 'vol1'>>**，并将其移动到*选定资源*区域。
3. 选择 **Exclude** 选项卡，选择 **Volume**，在 **Name contains** 字段中输入 **`vs1-dr`**，然后单击 **Add**。

   这排除了在 SVM "vs1-dr" 上为卷 "vol1" 生成的警报。
4. 单击*事件*并选择要应用于卷的事件。
5. 单击*操作*，然后在*提醒这些用户*字段中选择将接收警报电子邮件的用户的名称。
6. 配置此页面上用于发出 SNMP 陷阱和执行脚本的任何其他选项，然后单击 保存。

在 **Active IQ Unified Manager** 中查看警报

您可以从“警报设置”页面查看为各种事件创建的警报列表。还可以查看警报属性，例如警报描述、通知方法和频率、触发警报的事件、警报的电子邮件收件人以及受影响的资源（例如集群、聚合和卷）。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。

   警报列表显示在“警报设置”页面中。

在 **Active IQ Unified Manager** 中编辑警报

您可以编辑警报属性，例如与警报关联的资源、事件、收件人、通知选项、通知频率和关联脚本。

开始之前

您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。
2. 在*警报设置*页面中，选择要编辑的警报，然后单击*编辑*。
3. 在*编辑警报*对话框中，根据需要编辑名称、资源、事件和操作部分。

   您可以更改或删除与此警报关联的脚本。

4. 单击 **Save**。

删除 **Active IQ Unified Manager** 中的警报

您可以在不再需要时删除警报。例如，当特定资源不再受 Unified Manager 监控时，您可以删除为该资源创建的警报。

开始之前

您必须具有应用程序管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。
2. 在*警报设置*页面上，选择要删除的警报，然后单击*删除*。
3. 单击 是 确认删除请求。

警报窗口和对话框的说明

了解 **Active IQ Unified Manager** 中的"警报设置"页面

警报设置页面显示警报列表，并提供有关警报名称、状态、通知方法和通知频率的信息。您还可以从此页面添加、编辑、删除、启用或禁用警报。

您必须具有应用程序管理员或存储管理员角色。

命令按钮

- 添加

  显示用于添加新警报的“添加警报”对话框。

- 编辑

显示编辑警报对话框，用于编辑选定的警报。

- 删除

  删除选定的警报。

- 启用

  启用选定警报以发送通知。

- 禁用

  当您想要暂时停止发送通知时，禁用选定的警报。

- 测试

  测试选定警报，以在添加或编辑后验证其配置。

- 针对已解决和已废弃的事件发出的警报

  允许您在事件移动到“已解决”或“已过时”状态时启用或禁用发送警报。这可以帮助用户避免收到不必要的通知。

列表视图

列表视图以表格格式显示有关创建的警报的信息。您可以使用列筛选器自定义显示的数据。您还可以选择一个警报，以便在详细信息区域中查看有关该警报的更多信息。

- 状态

  指定警报是启用（）还是禁用（）。

- 警报

  显示警报的名称。

- 说明

  显示警报的说明。

- 通知方法

  显示为警报选择的通知方法。您可以通过电子邮件或 SNMP 陷阱通知用户。

- 通知频率

  指定管理服务器继续发送通知的频率（分钟），直到事件被确认、解决或移至“已过时”状态。

详细信息区域

详细信息区域提供有关所选警报的更多信息。

- 警报名称

显示警报的名称。

- 警报说明

  显示警报的说明。

- 事件

  显示要触发警报的事件。

- 资源

  显示要触发警报的资源。

- 包括

  显示要为其触发警报的资源组。

- 不包括

  显示不希望触发警报的资源组。

- 通知方法

  显示该警报的通知方法。

- 通知频率

  显示管理服务器继续发送警报通知的频率，直到事件被确认、解决或移至“已过时”状态。

- 脚本名称

  显示与所选警报关联的脚本的名称。生成警报时执行此脚本。

- 电子邮件收件人

  显示接收警报通知的用户的电子邮件地址。

了解 **Active IQ Unified Manager** 中的**"**添加警报**"**对话框

您可以创建警报以在生成特定事件时通知您，以便快速解决问题，从而最大限度地减少对环境的影响。您可以为单个资源或一组资源以及特定严重性类型的事件创建警报。您还可以指定警报的通知方法和频率。

您必须具有应用程序管理员或存储管理员角色。

名称

通过此区域，您可以指定警报的名称和描述：

- 警报名称

使您可以指定警报名称。

- 警报说明

  使您能够指定警报的描述。

资源

此区域允许您选择单个资源，或根据要为其触发警报的动态规则对资源进行分组。_动态规则_是根据您指定的文本字符串筛选出的一组资源。您可以通过从下拉列表中选择资源类型来搜索资源，也可以指定确切的资源名称以显示特定资源。

如果从任何存储对象详细信息页面创建警报，则存储对象将自动包含在警报中。

- 包括

  使您能够包含要为其触发警报的资源。您可以指定文本字符串来对与该字符串匹配的资源进行分组，并选择将此组包含在警报中。例如，您可以对名称包含“abc”字符串的所有卷进行分组。

- 排除

  使您能够排除不希望触发警报的资源。例如，您可以排除名称包含“xyz”字符串的所有卷。

  仅当您选择特定资源类型的所有资源时，才会显示“排除”选项卡：例如，<<All Volumes>> 或 <<All Volumes whose name contains 'xyz'>>。

  如果资源同时符合您指定的包含和排除规则，则排除规则优先于包含规则，并且不会为该事件生成警报。

事件

此区域可让您选择要为其创建警报的事件。您可以根据特定严重程度为事件创建警报，也可以为一组事件创建警报。

要选择多个事件，请在进行选择时按住 Ctrl 键。

- 事件严重程度

  使您能够根据严重程度类型选择事件，严重程度类型可以是“严重”、“错误”或“警告”。

- 事件名称包含

  使您能够选择名称包含指定字符的事件。

操作

通过此区域，您可以指定触发警报时要通知的用户。您还可以指定通知方法和通知频率。

- 提醒这些用户

  允许您指定要接收通知的用户的电子邮件地址或用户名。

  如果修改为用户指定的电子邮件地址并重新打开警报进行编辑，则“名称”字段将显示为空白，因为修改后的电子邮件地址不再映射到先前选择的用户。此外，如果已从“用户”页面修改所选用户的电子邮件地址，则不

会为所选用户更新已修改的电子邮件地址。

- 通知频率

  使您能够指定管理服务器在事件被确认、解决或移至过时状态之前发送通知的频率。

  您可以选择以下通知方法：

  - 仅通知一次
  - 以指定频率通知
  - 在指定时间范围内以指定频率发送通知

- 发出 **SNMP** 陷阱

  选中此框可指定是否应将 SNMP 陷阱发送到全局配置的 SNMP 主机。

- 执行脚本

  使您能够将自定义脚本添加到警报。此脚本在生成警报时执行。

> 如果在用户界面中看不到此功能，则是因为管理员已禁用此功能。如果需要，您可以从*存储管理* > *功能设置*启用此功能。

命令按钮

- 保存

  创建警报并关闭此对话框。

- 取消

  放弃更改并关闭对话框。

在 **Active IQ Unified Manager** 中编辑警报属性

您可以编辑警报属性，例如与警报关联的资源、事件、脚本和通知选项。

名称

通过此区域，您可以编辑警报的名称和描述。

- 警报名称

  使您可以编辑警报名称。

- 警报说明

  使您能够指定警报的描述。

- 警报状态

用于启用或禁用警报。

资源

此区域允许您选择单个资源，或根据要触发警报的动态规则对资源进行分组。您可以通过从下拉列表中选择资源类型来搜索资源，也可以指定确切的资源名称以显示特定资源。

- 包括

  使您能够包含要为其触发警报的资源。您可以指定文本字符串来对与该字符串匹配的资源进行分组，并选择要包含在警报中的此组。例如，您可以对名称包含 “vol0” 字符串的所有卷进行分组。

- 排除

  使您能够排除不希望触发警报的资源。例如，您可以排除名称包含“`xyz`”字符串的所有卷。

  仅当您选择特定资源类型的所有资源（例如，<<All Volumes>> 或 <<All Volumes whose name contains 'xyz'>>）时，“排除”选项卡才会显示。

事件

此区域可让您选择要触发警报的事件。您可以根据特定严重程度或针对一组事件触发事件警报。

- 事件严重程度

  使您能够根据严重程度类型选择事件，严重程度类型可以是“严重”、“错误”或“警告”。

- 事件名称包含

  使您能够选择名称包含指定字符的事件。

操作

通过此区域，您可以指定通知方法和通知频率。

- 提醒这些用户

  使您能够编辑电子邮件地址或用户名，或指定新电子邮件地址或用户名以接收通知。

- 通知频率

  使您能够编辑管理服务器发送通知的频率，直到事件被确认、解决或移至过时状态。

  您可以选择以下通知方法：

  - 仅通知一次
  - 以指定频率通知
  - 在指定时间范围内以指定频率发送通知

- 发出 **SNMP** 陷阱

  使您能够指定是否应将 SNMP 陷阱发送到全局配置的 SNMP 主机。

- 执行脚本

  使您能够将脚本与警报相关联。此脚本在生成警报时执行。

命令按钮

- 保存

  保存更改并关闭对话框。

- 取消

  放弃更改并关闭对话框。

管理脚本

在 **Active IQ Unified Manager** 中管理脚本

您可以使用脚本自动修改或更新 Unified Manager 中的多个存储对象。该脚本与警报相关联。当事件触发警报时，将执行脚本。您可以在生成警报时上传自定义脚本并测试其执行情况。

默认情况下，将脚本上传到 Unified Manager 并运行它们的功能处于启用状态。如果您的组织出于安全原因不想允许此功能，您可以从*存储管理* > *功能设置*禁用此功能。

相关信息

"启用和禁用上传脚本的功能"

脚本如何与 **Active IQ Unified Manager** 中的警报配合使用

您可以将警报与脚本关联，以便在 Unified Manager 中引发事件警报时执行脚本。您可以使用脚本来解决存储对象的问题或识别哪些存储对象正在生成事件。

在 Unified Manager 中为事件生成警报时，将向指定收件人发送警报电子邮件。如果您将警报与脚本相关联，则会执行脚本。您可以从警报电子邮件中获取传递给脚本的参数的详细信息。

如果您已创建自定义脚本并将其与特定事件类型的警报相关联，则将根据该事件类型的自定义脚本采取操作，默认情况下，“管理操作”页面或 Unified Manager 仪表板上的“修复它”操作不可用。

该脚本使用以下参数执行：

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`

- `-eventSourceType`
- `-eventState`
- `-eventArgs`

您可以在脚本中使用参数并收集相关事件信息或修改存储对象。

从脚本中获取参数的示例

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

生成警报时，系统将执行此脚本并显示以下输出：

```
-`eventID : 290`
-`eventSourceID : 4138`
```

在 **Active IQ Unified Manager** 中添加脚本

您可以在 Unified Manager 中添加脚本，并将脚本与警报相关联。这些脚本在生成警报时自动执行，使您能够获得有关为其生成事件的存储对象的信息。

开始之前

- 必须已创建并保存要添加到 Unified Manager 服务器的脚本。
- 支持的脚本文件格式有 Perl、Shell、PowerShell、Python 和 `.bat` 文件。

安装 **Unified Manager** 的平台	支持的语言
VMware	Perl 和 Shell 脚本
Linux	Perl、Python 和 Shell 脚本
Windows	PowerShell、Perl、Python 和 .bat 脚本

  - 对于 Perl 脚本，必须在 Unified Manager 服务器上安装 Perl。对于 VMware 安装，默认情况下会安装 Perl 5，脚本将仅支持 Perl 5 支持的内容。如果 Perl 是在 Unified Manager 之后安装的，则必须重新启动 Unified Manager 服务器。
  - 对于 PowerShell 脚本，必须在 Windows 服务器上设置相应的 PowerShell 执行策略，以便能够执行这些脚本。

> 如果您的脚本创建日志文件以跟踪警报脚本进度，则必须确保不会在 Unified Manager 安装文件夹中的任何位置创建日志文件。

- 您必须具有应用程序管理员或存储管理员角色。

您可以上传自定义脚本，并收集有关警报的事件详细信息。

如果在用户界面中看不到此功能，则是因为管理员已禁用此功能。如果需要，您可以从*存储管理* > *功能设置*启用此功能。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 脚本。
2. 在*脚本*页面中，单击*添加*。
3. 在*添加脚本*对话框中，单击*浏览*以选择您的脚本文件。
4. 输入选定脚本的说明。
5. 单击 **Add**。

相关信息

"启用和禁用上传脚本的功能"

删除 **Active IQ Unified Manager** 中的脚本

当脚本不再需要或有效时，您可以从 Unified Manager 中删除该脚本。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 此脚本不得与警报相关联。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 脚本。
2. 在*脚本*页面中，选择要删除的脚本，然后单击*删除*。
3. 在*警告*对话框中，单击*是*确认删除。

在 **Active IQ Unified Manager** 中执行测试脚本

您可以验证在针对存储对象生成警报后是否正确执行了您的脚本。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已将支持的文件格式的脚本上载到 Unified Manager。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 脚本。
2. 在*脚本*页面中，添加您的测试脚本。
3. 在左侧导航窗格中，单击*存储管理* > 警报设置。
4. 在*警报设置*页面中，执行以下操作之一：

目的	操作
添加警报	a. 单击 **Add**。 b. 在操作部分，将警报与测试脚本相关联。
编辑警报	a. 选择一个警报，然后单击*编辑*。 b. 在操作部分，将警报与测试脚本相关联。

5. 单击 **Save**。
6. 在*警报设置*页面中，选择您添加或修改的警报，然后单击*测试*。

   使用 "-test" 参数执行脚本，并向创建警报时指定的电子邮件地址发送通知警报。

了解受支持的 **Active IQ Unified Manager CLI** 命令

作为存储管理员，您可以使用 CLI 命令对存储对象执行查询，例如对群集、聚合、卷、qtree 和 LUN 执行查询。您可以使用 CLI 命令查询 Unified Manager 内部数据库和 ONTAP 数据库。您还可以在操作开始或结束时执行或在触发警报时执行的脚本中使用 CLI 命令。

所有命令前面都必须加上命令 `um cli login`以及用于身份验证的有效用户名和密码。

要运行 *um run* 命令，请确保您的帐户具有 *console* 应用程序访问权限。

CLI 命令	问题描述	输出
`um cli login -u <username> [-p <password>]`	登录 CLI。出于安全考虑，您应该只在“-u”选项后输入用户名。以这种方式使用时，系统将提示您输入密码，并且密码不会被捕获到历史记录或进程表中。会话在登录三小时后过期，之后用户必须重新登录。	显示相应的消息。
`um cli logout`	从 CLI 注销。	显示相应的消息。
`um help`	显示所有一级子命令。	显示所有一级子命令。
`um run cmd [ -t <timeout> ] <cluster> <command>`	在一个或多个主机上运行命令的最简单方法。主要用于警报脚本，以在 ONTAP 上获取或执行操作。可选的 timeout 参数设置命令在客户端上完成的最大时间限制（以秒为单位）。默认值为 0（永久等待）。	从 ONTAP 接收到的。
`um run query <sql command>`	执行 SQL 查询。仅允许从数据库读取的查询。不支持任何更新、插入或删除操作。	结果以表格形式显示。如果返回空集，或者存在任何语法错误或错误请求，则会显示相应的错误消息。

CLI 命令	问题描述	输出
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	将数据源添加到托管存储系统列表。数据源描述了如何建立与存储系统的连接。添加数据源时，必须指定选项 -u（用户名）和 -P（密码）。选项 -t（协议）指定用于与集群通信的协议（http 或 https）。如果未指定协议，则将尝试两种协议。选项 -p（端口）指定用于与集群通信的端口。如果未指定端口，则将尝试使用相应协议的默认值。此命令只能由存储管理员执行。	提示用户接受证书并打印相应的消息。
`um datasource list [ <datasource-id>]`	显示托管存储系统的数据源。	以表格格式显示以下值： `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message`。
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	修改一个或多个数据源选项。只能由存储管理员执行。	显示相应的消息。
`um datasource remove <datasource-id>`	从 Unified Manager 中删除数据源（集群）。	显示相应的消息。
`um option list [ <option> .. ]`	列出可使用 set 命令配置的所有选项。	以表格格式显示以下值： `Name, Value, Default Value, and Requires Restart.`
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	设置一个或多个选项。命令只能由存储管理员执行。	显示相应的消息。
`um version`	显示 Unified Manager 软件版本。	`Version ("9.6")`

CLI 命令	问题描述	输出
`um lun list [-q] [ -ObjectType <object-id>]`	列出筛选指定对象后的 LUN。-q 适用于所有命令，以不显示标头。ObjectType 可以是 lun、qtree、cluster、volume、quota 或 svm。 例如： **`um lun list -cluster 1`** 在此示例中，“-cluster” 是 objectType，“1” 是 objectId。该命令列出了 ID 为 1 的集群中的所有 LUN。	以表格格式显示以下值： `ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	列出对指定对象进行筛选后的存储虚拟机。ObjectType 可以是 lun、qtree、cluster、volume、quota 或 svm。 例如： **`um svm list -cluster 1`** 在此示例中，“-cluster” 是 objectType，“1” 是 objectId。该命令列出集群内 ID 为 1 的所有存储 VM。	以表格格式显示以下值： `Name and Cluster ID.`
`um qtree list [-q] [ -ObjectType <object-id>]`	列出筛选指定对象后的 qtree。-q 适用于所有不显示标头的命令。ObjectType 可以是 lun、qtree、cluster、volume、quota 或 svm。 例如： **`um qtree list -cluster 1`** 在此示例中，“-cluster” 是 objectType，“1” 是 objectId。该命令列出了 ID 为 1 的集群中的所有 qtree。	以表格格式显示以下值： `Qtree ID and Qtree Name.`

CLI 命令	问题描述	输出
`um disk list [-q] [-ObjectType <object-id>]`	列出对指定对象进行筛选后的磁盘。ObjectType 可以是磁盘、聚合、节点或集群。 例如： **`um disk list -cluster 1`** 在此示例中，“-cluster” 是 objectType，“1” 是 objectId。该命令列出了 ID 为 1 的集群中的所有磁盘。	以表格格式显示以下值 `ObjectType and object-id`。
`um cluster list [-q] [-ObjectType <object-id>]`	列出对指定对象进行筛选后的集群。ObjectType 可以是 disk、aggr、node、cluster、lun、qtree、volume、quota 或 svm。 例如： **`um cluster list -aggr 1`** 在此示例中，“-aggr”是 objectType，“1”是 objectId。该命令列出了 ID 为 1 的聚合所属的集群。	以表格格式显示以下值： `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key`。
`um cluster node list [-q] [-ObjectType <object-id>]`	在按指定对象筛选后列出集群节点。ObjectType 可以是 disk、aggr、node 或 cluster。 例如： **`um cluster node list -cluster 1`** 在此示例中，“-cluster” 为 objectType，“1” 为 objectId。该命令列出了 ID 为 1 的集群内的所有节点。	以表格格式显示以下值 `Name and Cluster ID`。
`um volume list [-q] [-ObjectType <object-id>]`	列出对指定对象进行筛选后的卷。ObjectType 可以是 lun、qtree、cluster、volume、quota、svm 或 aggregate。 例如： **`um volume list -cluster 1`** 在此示例中，“-cluster”是 objectType，“1”是 objectId。该命令列出了 ID 为 1 的集群内的所有卷。	以表格格式显示以下值 `Volume ID and Volume Name`。

CLI 命令	问题描述	输出
`um quota user list [-q] [-ObjectType <object-id>]`	列出筛选指定对象后的配额用户。ObjectType 可以是 qtree、cluster、volume、quota 或 svm。 例如： **`um quota user list -cluster 1`** 在此示例中，“-cluster” 是 objectType，“1” 是 objectId。该命令列出集群内 ID 为 1 的所有配额用户。	以表格格式显示以下值 `ID, Name, SID and Email`。
`um aggr list [-q] [-ObjectType <object-id>]`	列出对指定对象进行筛选后的聚合。ObjectType 可以是 disk、aggr、node、cluster 或 volume。 例如： **`um aggr list -cluster 1`** 在此示例中，“-cluster” 是 objectType，“1” 是 objectId。该命令列出了 ID 为 1 的集群内的所有聚合。	以表格格式显示以下值 `Aggr ID, and Aggr Name`。
`um event ack <event-ids>`	确认一个或多个事件。	显示相应的消息。
`um event resolve <event-ids>`	解决一个或多个事件。	显示相应的消息。
`um event assign -u <username> <event-id>`	将事件分配给用户。	显示相应的消息。
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	列出系统或用户生成的事件。根据源、状态和 ID 筛选事件。	以表格格式显示以下值 `Source, Source type, Name, Severity, State, User and Timestamp`。
`um backup restore -f <backup_file_path_and_name>`	使用 .7z 文件还原 MySQL 数据库备份。	显示相应的消息。

脚本窗口和对话框的说明

了解 **Active IQ Unified Manager** 中的脚本页面

您可以使用“脚本”页面将自定义脚本添加到 Unified Manager。您可以将这些脚本与警报相关联，以启用存储对象的自动重新配置。

您可以使用“脚本”页面在 Unified Manager 中添加或删除脚本。

命令按钮

- 添加

  显示用于添加脚本的“添加脚本”对话框。

- 删除

  删除选定脚本。

列表视图

列表视图以表格格式显示您添加到 Unified Manager 的脚本。

- 名称

  显示脚本的名称。

- 说明

  显示脚本说明。

在 **Active IQ Unified Manager** 中添加脚本对话框

“添加脚本”对话框使您可以将脚本添加到 Unified Manager。您可以使用脚本配置警报，以自动解决为存储对象生成的事件。

您必须具有应用程序管理员或存储管理员角色。

- 选择脚本文件

  使您能够为警报选择脚本。

- 说明

  使您能够指定脚本的说明。

监控和管理集群性能

Active IQ Unified Manager 性能监控简介

了解 Active IQ Unified Manager 中的性能监控

Active IQ Unified Manager（以前称为 OnCommand Unified Manager）为运行 NetApp ONTAP 软件的系统提供性能监控功能和事件根本原因分析。

Unified Manager 可帮助您识别过度使用集群组件并降低集群上其他工作负载性能的工作负载。通过定义性能阈值策略，您还可以为某些性能计数器指定最大值，以便在超出阈值时生成事件。Unified Manager 会提醒您这些性能事件，以便您可以采取纠正措施，并将性能恢复到正常运行水平。您可以在 Unified Manager UI 中查看和分析事件。

Unified Manager 可监控两种类型工作负载的性能：

- 用户定义的工作负载

  这些工作负载由您在集群中创建的 FlexVol 卷和 FlexGroup 卷组成。

- 系统定义的工作负载

  这些工作负载包括内部系统活动。

探索 Active IQ Unified Manager 性能监控功能

Unified Manager 从运行 ONTAP 软件的系统收集和分析性能统计数据。它使用动态性能阈值和用户定义的性能阈值来监控许多集群组件上的各种性能计数器。

高响应时间（延迟）表明存储对象（例如卷）的运行速度低于正常水平。此问题还表明使用该卷的客户端应用程序的性能已下降。Unified Manager 确定性能问题所在的存储组件，并提供您可以采取的建议操作列表，以解决该性能问题。

Unified Manager 包括以下功能：

- 监控和分析来自运行 ONTAP 软件的系统的工作负载性能统计数据。
- 跟踪群集、节点、聚合、端口、SVM、卷、LUN、NVMe 命名空间和网络接口（LIF）的性能计数器。
- 显示绘制一段时间内工作负载活动的详细图表；包括 IOPS（操作）、MB/s（吞吐量）、延迟（响应时间）、利用率、性能容量和缓存比率。
- 使您能够创建用户定义的性能阈值策略，以便在超出阈值时触发事件并发送电子邮件警报。
- 使用系统定义的阈值和动态性能阈值来学习您的工作负载活动，以识别并提醒您注意性能问题。
- 标识应用于您的卷和 LUN 的服务质量 (QoS) 策略和性能服务级别策略 (PSL)。
- 清楚地识别处于争用状态的集群组件。
- 识别过度使用集群组件的工作负载，以及性能受活动增加影响的工作负载。

使用 **Active IQ Unified Manager** 接口管理存储系统性能

这些部分包含有关 Active IQ Unified Manager 为解决数据存储容量、可用性和保护问题而提供的两个用户界面的信息。这两个 UI 是 Unified Manager Web UI 和维护控制台。

如果要在 Unified Manager 中使用保护功能，还必须安装和配置 OnCommand Workflow Automation (WFA)。

Unified Manager Web UI

Unified Manager Web UI 使管理员能够监控与数据存储容量、可用性和保护相关的集群问题并对其进行故障排除。

这些部分介绍了管理员可以遵循的一些常见工作流程，以便对 Unified Manager Web UI 中显示的存储容量、数据可用性或保护问题进行故障排除。

维护控制台

Unified Manager 维护控制台使管理员能够监视、诊断和解决与 Unified Manager 服务器本身相关的操作系统问题、版本升级问题、用户访问问题和网络问题。如果 Unified Manager Web UI 不可用，则维护控制台是访问 Unified Manager 的唯一方式。

您可以使用此信息访问维护控制台并使用它来解决与 Unified Manager 服务器功能相关的问题。

在 **Active IQ Unified Manager** 中查看集群配置和性能数据

_集群配置数据_的收集间隔为 15 分钟。例如，添加集群后，需要 15 分钟才能在 Unified Manager UI 中显示集群详细信息。对集群进行更改时，此间隔也适用。

例如，如果将两个新卷添加到集群中的 SVM，则在下一个轮询间隔（可能长达 15 分钟）之后，UI 中会看到这些新对象。

Unified Manager 每五分钟从所有受监控的集群中收集当前的 性能统计信息。它分析这些数据以识别性能事件和潜在问题。它保留 30 天的五分钟历史性能数据和 180 天的一小时历史性能数据。这使您能够查看当月非常精细的性能详细信息，以及长达一年的一般性能趋势。

收集轮询偏移了几分钟，因此不会同时发送来自每个集群的数据，这可能会影响性能。

下表介绍了 Unified Manager 执行的收集活动：

活动	时间间隔	问题描述
性能统计轮询	每 5 分钟	从每个集群收集实时性能数据。
统计分析	每 5 分钟	每次统计轮询后，Unified Manager 都会将收集的数据与用户定义、系统定义和动态阈值进行比较。 如果已违反任何性能阈值，Unified Manager 将生成事件并向指定用户发送电子邮件（如果已配置）。

活动	时间间隔	问题描述
配置轮询	每 15 分钟	从每个集群收集详细的清单信息，以识别所有存储对象（节点、SVM、卷等）。
总结	每小时	将最新的 12 个五分钟性能数据收集汇总为每小时平均值。 每小时平均值用于一些 UI 页面，并保留 180 天。
预测分析和数据修剪	每天午夜后	分析集群数据，为未来 24 小时的卷延迟和 IOPS 建立动态阈值。 从数据库中删除任何超过 30 天的五分钟性能数据。
数据修剪	每天凌晨 2 点后	从数据库中删除任何超过 180 天的事件和超过 180 天的动态阈值。
数据修剪	每天凌晨 3:30 后	从数据库中删除任何超过 180 天的一小时性能数据。

了解 **Active IQ Unified Manager** 中的数据连续性收集周期

数据连续性收集周期将在默认情况下每五分钟运行一次的实时集群性能收集周期之外检索性能数据。数据连续性收集使 Unified Manager 能够填补无法收集实时数据时出现的统计数据空缺。

当发生以下事件时，Unified Manager 将对历史性能数据执行数据连续性收集轮询：

- 集群最初被添加到 Unified Manager。

  Unified Manager 收集过去 15 天的历史性能数据。这使您能够在添加集群几个小时后查看集群的两周历史性能信息。

  此外，如果存在系统定义的阈值事件，则报告上一期间的事件。

- 当前性能数据收集周期未按时完成。

  如果实时性能轮询超过了五分钟的收集周期，则会启动数据连续性收集周期以收集缺失的信息。如果没有数据连续性收集，则会跳过下一个收集周期。

- Unified Manager 已无法访问一段时间，然后重新上线，如以下情况所示：
  - 它已重新启动。
  - 它在软件升级或创建备份文件时被关闭。
  - 修复了网络中断。
- 某个集群在一段时间内无法访问，然后重新上线，如以下情况所示：
  - 修复了网络中断。

◦ 缓慢的广域网连接延迟了性能数据的正常收集。

数据连续性收集周期最多可收集 24 小时的历史数据。如果 Unified Manager 停机时间超过 24 小时，UI 页面中会出现性能数据缺失。

数据连续性采集周期和实时数据采集周期不能同时运行。数据连续性采集周期必须在启动实时性能数据采集之前完成。当需要数据连续性采集来收集超过一小时的历史数据时，您会在“通知”窗格顶部看到该集群的横幅消息。

了解 Active IQ Unified Manager 中收集的数据和事件中的时间戳

显示在收集的运行状况和性能数据中的时间戳，或显示为事件的检测时间的时间戳，基于 ONTAP 集群时间，并调整为 Web 浏览器上设置的时区。

强烈建议您使用网络时间协议（NTP）服务器来同步 Unified Manager 服务器、ONTAP 群集和 Web 浏览器上的时间。

如果您看到特定集群的时间戳看起来不正确，则可能需要检查集群时间是否已正确设置。

在 Unified Manager GUI 中导航性能工作流

在 Active IQ Unified Manager GUI 中导航性能工作流

Unified Manager 界面提供了许多用于收集和显示性能信息的页面。您可以使用左侧导航面板导航到 GUI 中的页面，并使用页面上的选项卡和链接查看和配置信息。

您可以使用以下所有页面来监控集群性能信息并进行故障排除：

- 控制面板页面
- 存储和网络对象清单页面
- 存储对象详细信息页面（包括性能资源管理器）
- 配置和设置页面
- 事件页面

登录到 Active IQ Unified Manager UI

您可以使用支持的 Web 浏览器登录到 Unified Manager UI。

开始之前

- Web 浏览器必须满足最低要求。

  请参见 "mysupport.netapp.com/cn/matrix"中的互操作性表，获取支持的浏览器版本的完整列表。

- 您必须具有 Unified Manager 服务器的 IP 地址或 URL。

不活动 1 小时后，您将自动退出会话。此时间范围可以在 常规 > 功能设置 下配置。

步骤

1. 在 Web 浏览器中输入 URL，其中 URL 是 Unified Manager 服务器的 IP 地址或完全限定域名（FQDN）：
   - 对于 IPv4： `https://URL/`
   - 对于 IPv6： `https://[URL]/`

如果服务器使用自签名数字证书，浏览器可能会显示警告，指示证书不受信任。您可以确认风险以继续访问，或者安装证书颁发机构（CA）签名的数字证书以进行服务器身份验证。。在登录屏幕上，输入您的用户名和密码。

如果使用 SAML 身份验证保护对 Unified Manager 用户界面的登录，您将在身份提供程序（IdP）登录页面而不是 Unified Manager 登录页面中输入凭据。

将显示 Dashboard 页面。

如果 Unified Manager 服务器尚未初始化，新的浏览器窗口将显示首次使用向导。您必须输入用于接收电子邮件警报的初始收件人电子邮件地址、负责处理电子邮件通信的 SMTP 服务器，以及是否启用 AutoSupport 以将您的 Unified Manager 安装信息发送给技术支持。完成上述信息填写后，Unified Manager 用户界面将会显示。

图形界面和导航路径

探索 **Active IQ Unified Manager** 中的图形界面和导航路径

Unified Manager 具有极大的灵活性，使您能够以各种方式完成多项任务。在 Unified Manager 中工作时，您会发现许多导航路径。虽然无法显示所有可能的导航组合，但您应该熟悉一些更常见的场景。

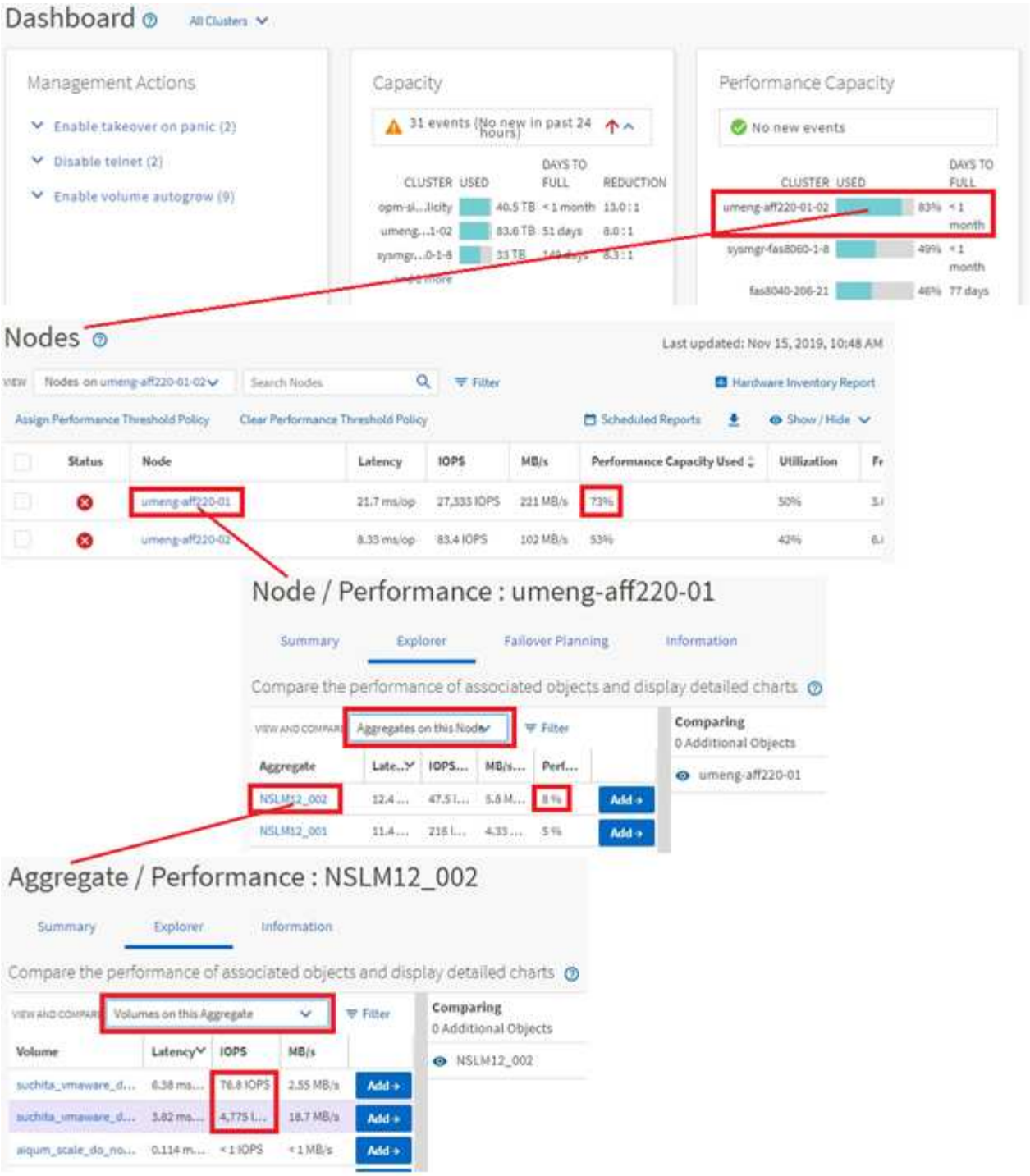
在 **Active IQ Unified Manager** 中监控集群对象导航

您可以监控由 Unified Manager 管理的任何集群中所有对象的性能。监控存储对象可为您提供集群和对象性能的概述，并包括性能事件监控。您可以在高级别查看性能和事件，也可以进一步调查对象性能和性能事件的任何详细信息。

这是许多可能的集群对象导航的一个示例：

1. 在“仪表板”页面中，查看“性能容量”面板中的详细信息，以确定使用最多性能容量的集群，然后单击条形图以导航到该集群的节点列表。
2. 识别具有最高性能容量使用值的节点，然后单击该节点。
3. 从节点/性能资源管理器页面，单击查看和比较菜单中的*此节点上的聚合*。
4. 确定使用性能容量最多的聚合，然后单击该聚合。
5. 从聚合/性能资源管理器页面，单击查看和比较菜单中的*此聚合上的卷*。
6. 确定使用 IOPS 最多的卷。

您应该调查这些卷，以确定是否应该应用 QoS 策略或性能服务级别策略，或更改策略设置，以便这些卷不会在集群上使用如此大的 IOPS 百分比。



监控 **Active IQ Unified Manager** 中的集群性能导航

您可以监控由 Unified Manager 管理的所有集群的性能。监控您的集群可为您提供集群和对象性能的概述，并包括性能事件监控。您可以在高级别查看性能和事件，也可以进一步调查集群和对象性能以及性能事件的任何详细信息。

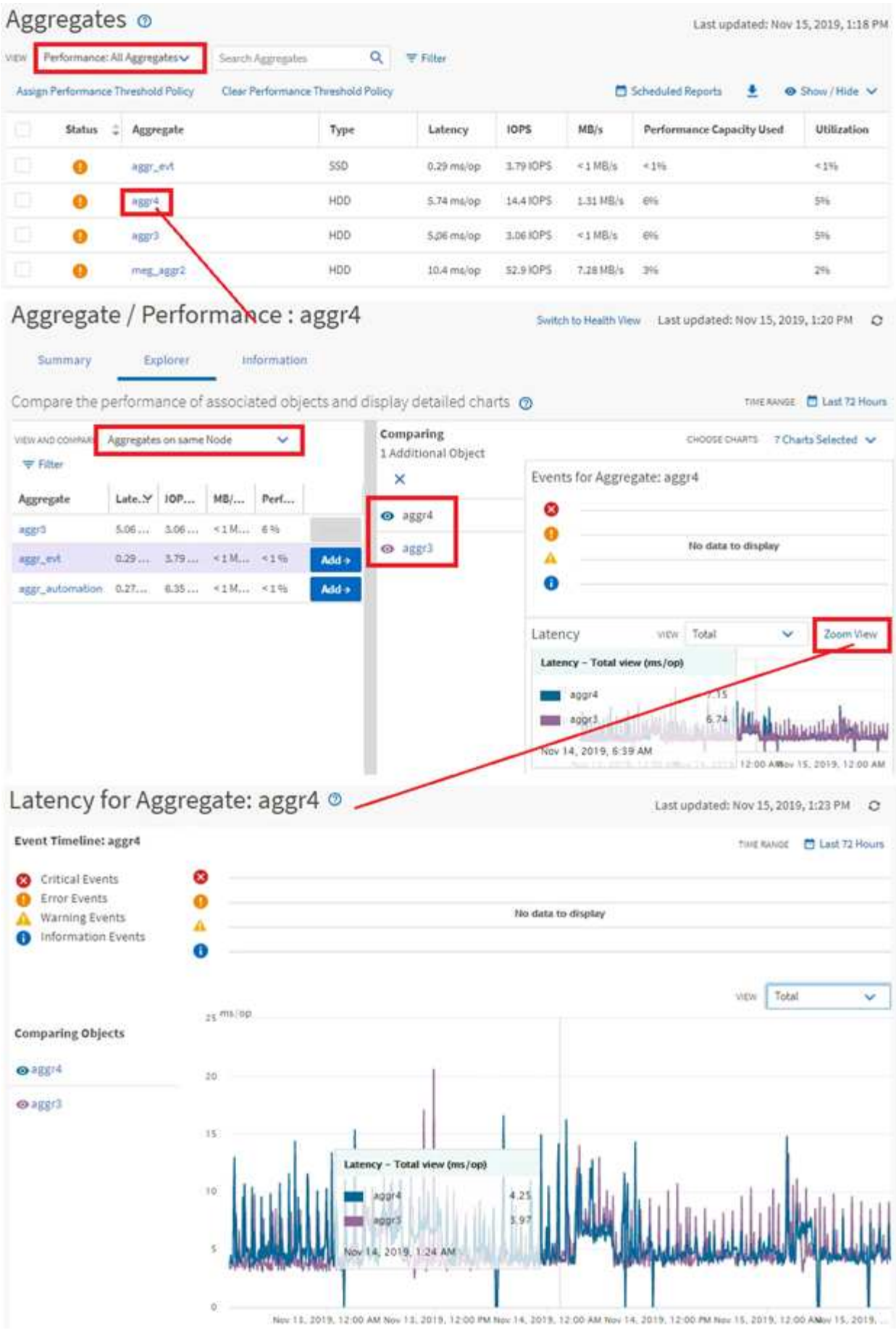
这是许多可能的集群性能导航路径的一个示例：

1. 在左侧导航窗格中，单击*存储* > 聚合。
2. 要查看这些聚合中的性能信息，请选择“性能：所有聚合”视图。

3. 确定要调查的聚合，然后单击该聚合名称以导航到“聚合/性能资源管理器”页面。
4. （可选）在“查看和比较”菜单中选择要与此聚合进行比较的其他对象，然后将其中一个对象添加到比较窗格。

   两个对象的统计数据将显示在计数器图表中进行比较。

5. 在资源管理器页面右侧的“比较”窗格中，单击其中一个计数器图表中的*缩放视图*可查看该聚合的性能历史记录的详细信息。


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
aggr4
aggr3
CHOOSE CHARTS
7 Charts Selected
Events for Aggregate: aggr4
No data to display
Latency
VIEW
Total
Zoom View
Latency – Total view (ms/op)
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
25
ms/op
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,

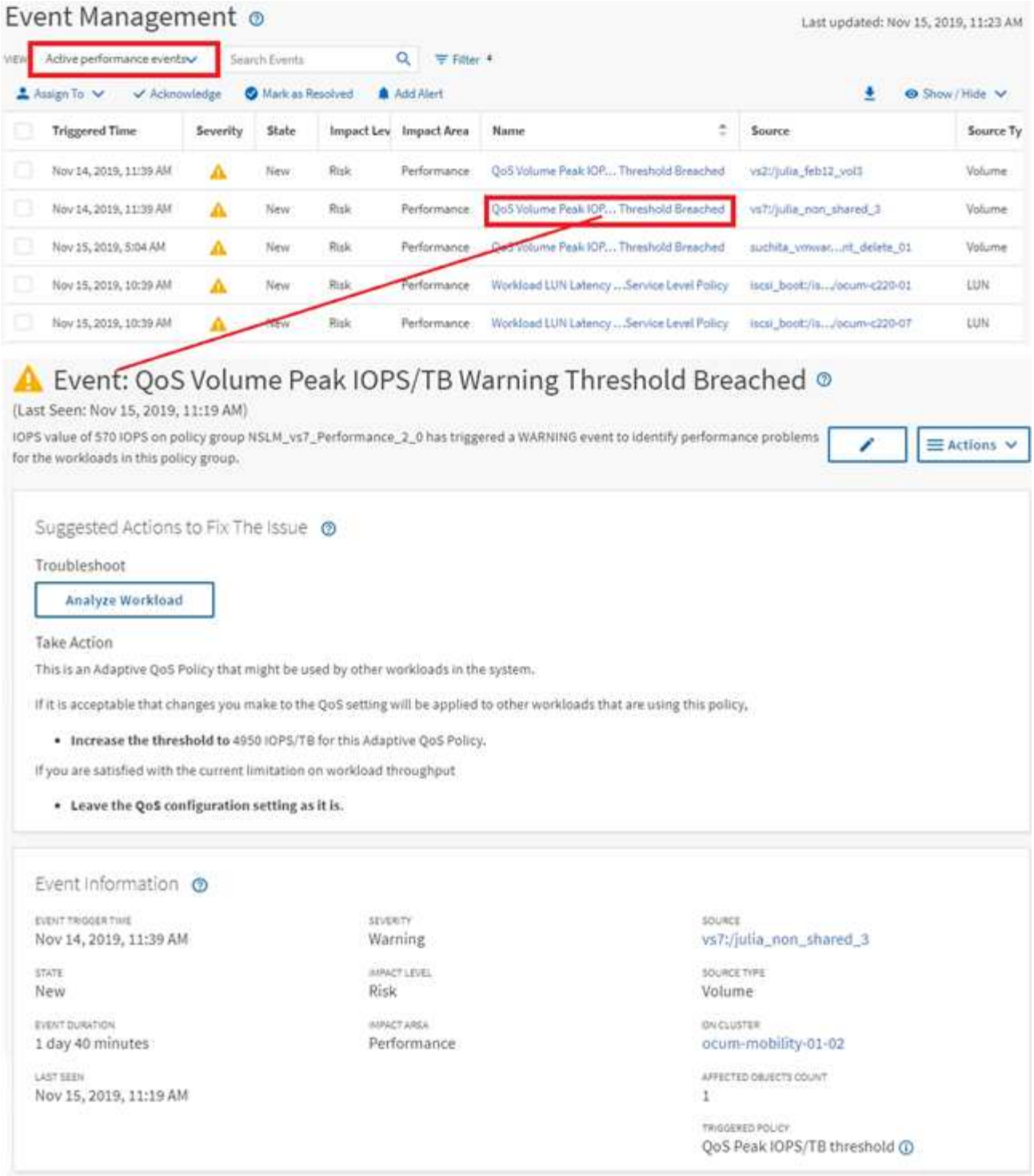
Unified Manager 事件详细信息页面可让您深入了解任何性能事件。这在调查性能事件、进行故障排除以及微调系统性能时非常有用。

根据性能事件的类型，您可能会看到两种类型的事件详细信息页面之一：

- 用户定义和系统定义的阈值策略事件的事件详细信息页面
- 动态阈值策略事件的事件详细信息页面

这是事件调查导航的一个示例。

1. 在左侧导航窗格中，单击*事件管理*。
2. 在“视图”菜单中，单击 **Active performance events**。
3. 单击要调查的事件名称，系统将显示事件详情页面。
4. 查看事件的描述并查看建议操作（如有），查看可帮助您解决问题的事件的更多详细信息。您可以单击*分析工作负载*按钮，显示详细的性能图表，以帮助进一步分析问题。



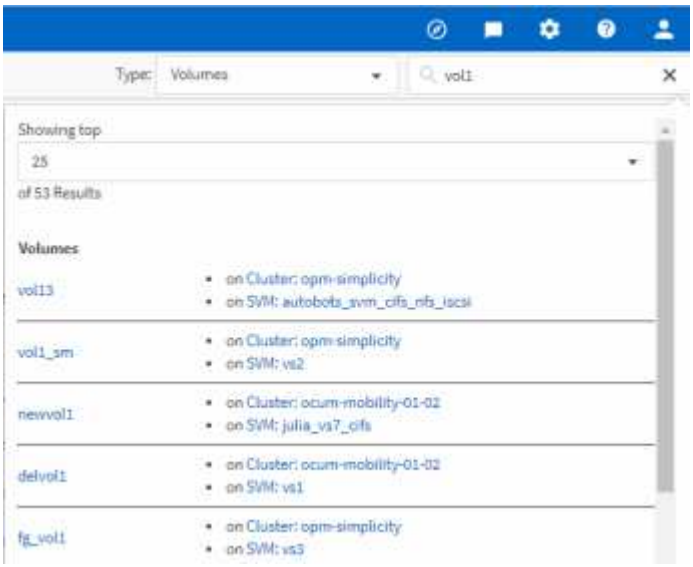
在 **Active IQ Unified Manager** 中搜索存储对象

您可以使用菜单栏顶端的*搜索所有存储对象*字段快速访问特定对象。这种对所有对象进行全局搜索的方法使您能够按类型快速定位特定对象。搜索结果按存储对象类型排序，您可以使用下拉菜单进行筛选。有效的搜索必须至少包含三个字符。

全局搜索显示结果总数，但只有前 25 个搜索结果可供访问。因此，如果您知道要快速查找的项目，则可以将全局搜索功能视为查找特定项目的快捷方式工具。对于完整的搜索结果，您可以使用对象清单页面中的搜索及其相关的筛选功能。

您可以单击下拉框并选择 全部 以同时搜索所有对象和事件。或者，您可以单击下拉框来指定对象类型。在 搜索所有存储对象 字段中至少输入三个字符的对象或事件名称，然后按 **Enter** 键显示搜索结果，例如：

- 集群：集群名称
- 节点：节点名称
- 聚合：聚合名称
- SVM：SVM 名称
- 卷：卷名
- LUN：LUN 路径



LIF 和端口在全局搜索栏中不可搜索。

在此示例中，下拉框选择了 Volume 对象类型。在 **Search all Storage Objects** 字段中键入“`vol`”将显示名称包含这些字符的所有卷的列表。对于对象搜索，您可以单击任何搜索结果以导航到该对象的“性能资源管理器”页面。对于事件搜索，单击搜索结果中的项目将导航到“事件详细信息”页面。

在 **Active IQ Unified Manager** 中筛选清单页面内容

您可以在 Unified Manager 中筛选清单页面数据，以根据特定条件快速查找数据。您可以使用筛选功能来缩小 Unified Manager 页面的内容范围，以仅显示您感兴趣的结果。这提供了一种非常有效的方法，仅显示您感兴趣的数据。

使用 过滤 根据您的偏好自定义网格视图。可用的过滤器选项基于在网格中查看的对象类型。如果当前已应用过滤器，则已应用过滤器的数量将显示在“过滤器”按钮的右侧。

支持三种类型的过滤器参数。

参数	验证
字符串（文本）	运算符是*包含*、以.....开头、以.....结尾*和*不包含。

参数	验证
数字	运算符包括*大于*、小于、在最后*和*之间。
枚举（文本）	运算符是 **is** 和 **is not**。

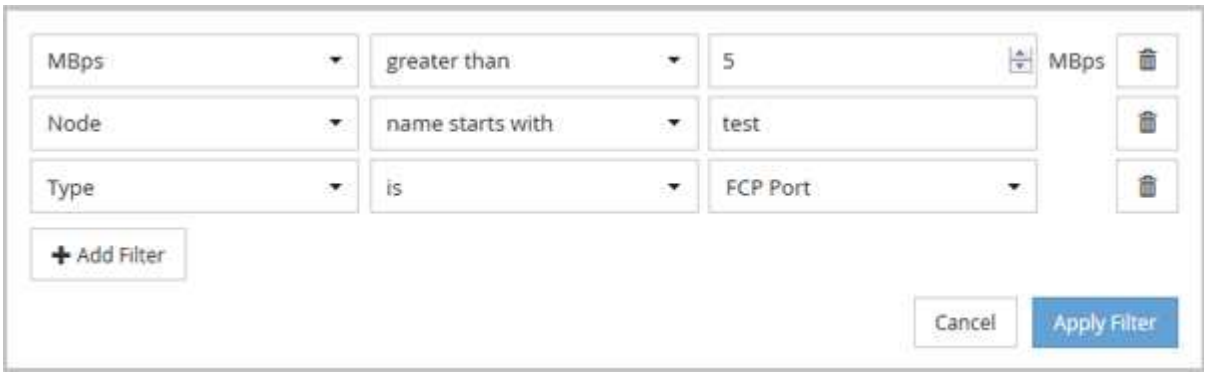
每个筛选器都需要 Column（列）、Operator（运算符）和 Value（值）字段；可用的筛选器反映当前页面上的可筛选列。您最多可以应用四个筛选器。筛选结果基于组合的筛选器参数。筛选结果适用于筛选搜索中的所有页面，而不仅仅是当前显示的页面。

您可以使用“过滤”面板添加过滤器。

1. 在页面顶部，单击*筛选*按钮。此时将显示筛选面板。
2. 单击左侧下拉列表并选择一个对象；例如，*Cluster* 或性能计数器。
3. 单击中部下拉列表，然后选择要使用的运算符。
4. 在最后一个列表中，选择或输入一个值以完成此对象的筛选器。
5. 要添加其他过滤器，请单击 **+**添加过滤器。此时将显示一个额外的过滤器字段。使用前述步骤中描述的过程完成此过滤器。请注意，添加第四个过滤器后，**+**添加过滤器 按钮不再显示。
6. 单击*应用过滤器*。过滤器选项将应用于网格，过滤器的数量将显示在“过滤器”按钮的右侧。
7. 使用“筛选”面板，通过单击要删除的筛选器右侧的垃圾箱图标来删除单个筛选器。
8. 要删除所有过滤器，请点击过滤面板底部的*重置*。

筛选示例

该图显示了带有三个筛选条件的“筛选”面板。当您的筛选条件少于最多四个时，会显示 **+**添加筛选条件 按钮。



单击 应用过滤器 后，过滤面板将关闭，应用您的过滤器，并显示已应用的过滤器数量（ 3 ）。

从仪表板监控集群性能

通过 **Active IQ Unified Manager** 中的信息板监控集群性能

Unified Manager 仪表板提供了几个面板，显示由此 Unified Manager 实例监控的所有集群的高级别性能状态。它使您能够评估受管集群的整体性能，并快速记录、定位或分配任何已识别的特定事件以解决问题。

查看 **Active IQ Unified Manager** 控制面板上的性能面板

Unified Manager 仪表板提供了几个面板，显示环境中正在受监控的所有集群的高级性能状态。您可以选择查看所有集群或单个集群的状态。

除了显示性能信息外，大多数面板还显示该类别中活动事件的数量，以及过去 24 小时内添加的新事件的数量。这些信息有助于您确定可能需要进一步分析哪些集群以解决报告的事件。单击事件将显示前几个事件，并提供指向事件管理清单页面的链接，该页面已过滤以显示该类别中的事件。

以下面板提供性能状态。

- 性能容量面板

  在查看所有群集时，此面板显示每个群集的性能容量值（过去 1 小时的平均值）以及直到性能容量达到上限的天数（基于每日增长率）。单击条形图将转到该群集的节点清单页面。请注意，节点清单页面显示过去 72 小时的平均性能容量，因此该值可能与仪表板值不匹配。

  查看单个集群时，此面板显示集群性能容量、总 IOPS 和总吞吐量值。

- 工作负载 **IOPS** 面板

  启用工作负载活动管理并查看单个集群时，此面板将显示当前在特定 IOPS 范围内运行的工作负载总数。

- 工作负载性能面板

  启用工作负载活动管理后，此面板将显示分配给每个定义的性能服务级别的符合和不符合工作负载的总数。单击条形图将转到“工作负载”页面中分配给该策略的工作负载。

- 使用概览面板

  查看所有集群时，您可以选择查看按最高 IOPS 或吞吐量 (MB/s) 排序的集群。

  在查看单个集群时，您可以选择查看该集群上的工作负载，并按最高 IOPS 或吞吐量（MB/s）进行排序。

解释 **Active IQ Unified Manager** 中的性能横幅消息

Unified Manager 可能会在通知页面（来自通知铃）上显示横幅消息，提醒您注意特定集群的状态问题。

横幅消息	问题描述	解决方法
`No performance data is being collected from cluster cluster_name. Restart Unified Manager to correct this issue.`	Unified Manager 收集服务已停止，并且未从任何集群收集任何性能数据。	重新启动 Unified Manager 以更正此问题。如果无法解决问题，请联系技术支持。

横幅消息	问题描述	解决方法
`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.`	当前正在运行数据连续性收集周期以检索实时集群性能收集周期之外的性能数据。	无需执行操作。在数据连续性收集周期完成后将收集当前性能数据。 当添加新集群或 Unified Manager 由于某种原因无法收集当前性能数据时，将运行数据连续性收集周期。

在 **Active IQ Unified Manager** 中更改性能统计信息收集间隔

性能统计的默认收集间隔为 5 分钟。如果发现大型集群的收集未在默认时间内完成，则可以将此时间间隔更改为 10 或 15 分钟。此设置会影响此 Unified Manager 实例正在监控的所有集群的统计信息收集。

开始之前

您必须拥有已授权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。

性能统计数据收集未按时完成的问题由横幅消息 `Unable to consistently collect from cluster <cluster_name>`或 `Data collection is taking too long on cluster <cluster_name>`指示。

只有在因统计信息收集问题而需要时，才应更改收集间隔。请勿出于任何其他原因更改此设置。

> 将此值从默认设置 5 分钟更改后，可能会影响 Unified Manager 报告的性能事件的数量和频率。例如，当超出策略 30 分钟时，系统定义的性能阈值会触发事件。使用 5 分钟收集时，必须连续六次收集超出策略。对于 15 分钟的收集，只需在两个收集期内超出策略即可。

集群设置页面底部的消息指示当前统计数据收集间隔。

步骤

1. 使用 SSH 作为维护用户登录到 Unified Manager 主机。

   此时将显示 Unified Manager 维护控制台提示。

2. 键入标记为*性能轮询间隔配置*的菜单选项的编号，然后按 Enter。
3. 如果出现提示，请再次输入维护用户密码。
4. 键入要设置的新轮询间隔的数值，然后按 Enter 键。

如果您将 Unified Manager 收集时间间隔更改为 10 或 15 分钟，并且当前连接到外部数据提供程序（如 Graphite），则必须更改数据提供程序传输时间间隔，使其等于或大于 Unified Manager 收集时间间隔。

使用工作负载分析器排除工作负载故障

使用 **Active IQ Unified Manager** 中的工作负载分析器对工作负载进行故障排除

工作负载分析器提供了一种方法，可以在单个页面上查看单个工作负载的重要运行状况和性能标准，以帮助进行故障排除。通过查看工作负载的所有当前和过去事件，您可以更好

地了解为什么工作负载现在可能存在性能或容量问题。

使用此工具还可以帮助您确定存储是否是应用程序任何性能问题的原因，或者该问题是否由网络或其他相关问题引起。

您可以从用户界面中的多个位置启动此功能：

- 从左侧导航菜单上的工作负载分析选项中
- 在事件详细信息页面中，单击*分析工作负载*按钮
- 从任何工作负载清单页面（卷、LUN、工作负载、NFS 共享或 SMB/CIFS 共享），单击更多图标 ⋮，然后单击 分析工作负载
- 从 Virtual Machines 页面，通过单击任意 Datastore 对象中的 **Analyze Workload** 按钮

当您从左侧导航菜单启动该工具时，您可以输入要分析的任何工作负载的名称，并选择要进行故障排除的时间范围。当您从任何工作负载或虚拟机清单页面启动该工具时，系统会自动填写工作负载的名称，并以默认的 2 小时时间范围显示工作负载的数据。当您从事件详细信息页面启动该工具时，系统会自动填写工作负载的名称，并显示 10 天的数据。

了解 **Active IQ Unified Manager** 中的工作负载分析器数据

工作负载分析器页面显示有关可能影响工作负载的任何当前事件的信息、可能解决导致事件的问题的建议以及用于分析性能和容量历史记录的图表。

在页面顶部，指定要分析的工作负载（卷或 LUN）的名称以及要查看统计信息的时间范围。如果您想查看更短或更长的时间段，可以随时更改时间范围。

页面的其他区域显示分析结果以及性能和容量图表。

ⓘ LUN 的工作负载图表无法提供与卷图表相同级别的统计信息，因此在分析这两种类型的工作负载时，您会注意到差异。

- 事件摘要区域

  显示在一段时间内发生的事件数量和类型的简要概述。当存在来自不同影响领域（例如性能和容量）的事件时，将显示此信息，以便您可以选择感兴趣的事件类型的详细信息。单击事件类型可查看事件名称列表。

  如果在时间范围内只有一个事件，则会列出针对某些事件的解决问题的建议列表。

- 事件时间表

  显示指定时间范围内发生的所有事件。将光标悬停在每个事件上以查看事件名称。

  如果您通过单击“事件详细信息”页面中的 分析工作负载 按钮到达此页面，则选定事件的图标会显得更大，以便您识别该事件。

- 性能图表区域

  根据所选时间范围显示延迟、吞吐量（IOPS 和 MB/s）和利用率（节点和聚合）的图表。如果要执行进一步分析，可以单击“查看性能详细信息”链接以显示工作负载的“性能资源管理器”页面。

- *延迟*显示所选时间范围内工作负载的延迟。该图表有三个视图，使您能够查看：
  - *总计*延迟
  - *细分*延迟（按读取、写入和其他进程细分）
  - *集群组件*延迟（按集群组件细分）

有关此处显示的集群组件的说明，请参阅 "集群组件及其可能出现争用的原因"。 吞吐量*显示所选时间范围内工作负载的 **IOPS** 和 **MB/s** 吞吐量。该图表具有四个视图，可让您查看： 总计*吞吐量 细分*吞吐量（按读取、写入和其他进程分列） 云吞吐量（用于向云写入数据和从云读取数据的 MB/s；对于将容量分层到云的工作负载） * 带预测的 **IOPS**（预测在时间范围内预期的上限和下限 **IOPS** 吞吐量值）此图表还显示服务质量（**QoS**）最大和最小吞吐量阈值设置（如果已配置），因此您可以查看系统可能有意使用 **QoS** 策略限制吞吐量的位置。 *利用率*显示在选定时间范围内运行此工作负载的聚合和节点的利用率。从这里，您可以看到您的聚合或节点是否被过度利用，从而可能导致高延迟。分析 FlexGroup 卷时，利用率图表上列出了多个节点和多个聚合。

- 容量图表区域

  显示工作负载过去一个月的数据容量和 Snapshot 容量图表。

  对于卷，如果要执行进一步分析，可以单击“查看容量详细信息”链接以显示工作负载的“运行状况详细信息”页面。LUN 不提供此链接，因为没有 LUN 的运行状况详细信息页面。

  - *容量视图*显示分配给工作负载的总可用空间和逻辑已用空间（在所有 NetApp 优化之后）。
  - *快照视图*显示为快照副本预留的总空间以及当前使用的空间量。请注意，LUN 不提供快照视图。
  - *云层视图*显示本地性能层使用的容量以及云层使用的容量。这些图表包括此工作负载的容量已满之前剩余时间的估计值。此信息基于历史使用情况，至少需要 10 天的数据。当剩余容量少于 30 天时，Unified Manager 会将存储标识为“`几乎已满\`”。

了解何时在 **Active IQ Unified Manager** 中使用工作负载分析器

您通常会使用工作负载分析器对用户报告的延迟问题进行故障排除，更全面地分析报告的事件或警报，或者探索您发现运行异常的工作负载。

如果用户联系您说他们正在使用的应用程序运行非常缓慢，您可以检查应用程序正在运行的工作负载的延迟、吞吐量和利用率图表，以查看存储是否是性能问题的原因。您也可以使用容量图表查看容量是否较低，因为容量使用率超过 85% 的 ONTAP 系统可能会导致性能问题。这些图表将帮助您确定问题是由存储还是由网络或其他相关问题引起的。

如果 Unified Manager 已生成性能事件，并且您希望更彻底地查看问题的原因，则可以通过单击 分析工作负载 按钮从事件详细信息页面启动工作负载分析器，以研究工作负载的一些延迟、吞吐量和容量趋势。

如果您在查看任何工作负载清单页面（卷、LUN、工作负载、NFS 共享或 SMB/CIFS 共享）时发现工作负载似乎运行异常，则可以单击更多图标 ⋮，然后单击 分析工作负载 打开工作负载分析页面以进一步检查工作负载。

在 **Active IQ Unified Manager** 中使用工作负载分析器

从用户界面启动工作负载分析器的方法有很多。在这里，我们将介绍从左侧导航窗格启动该工具。

步骤

1. 在左侧导航窗格中，单击*工作负载分析*。

   此时将显示工作负载分析页面。

2. 如果您知道工作负载名称，请输入名称。如果您不确定全名，请输入至少 3 个字符，系统将显示与字符串匹配的工作负载列表。
3. 如果要查看超过默认 2 小时的统计数据，请选择时间范围，然后单击*应用*。
4. 查看摘要区域以查看在时间范围内发生的事件。
5. 查看性能和容量图表，了解任何指标何时出现异常，并查看是否有任何事件与异常条目一致。

从性能集群登录页面监控集群性能

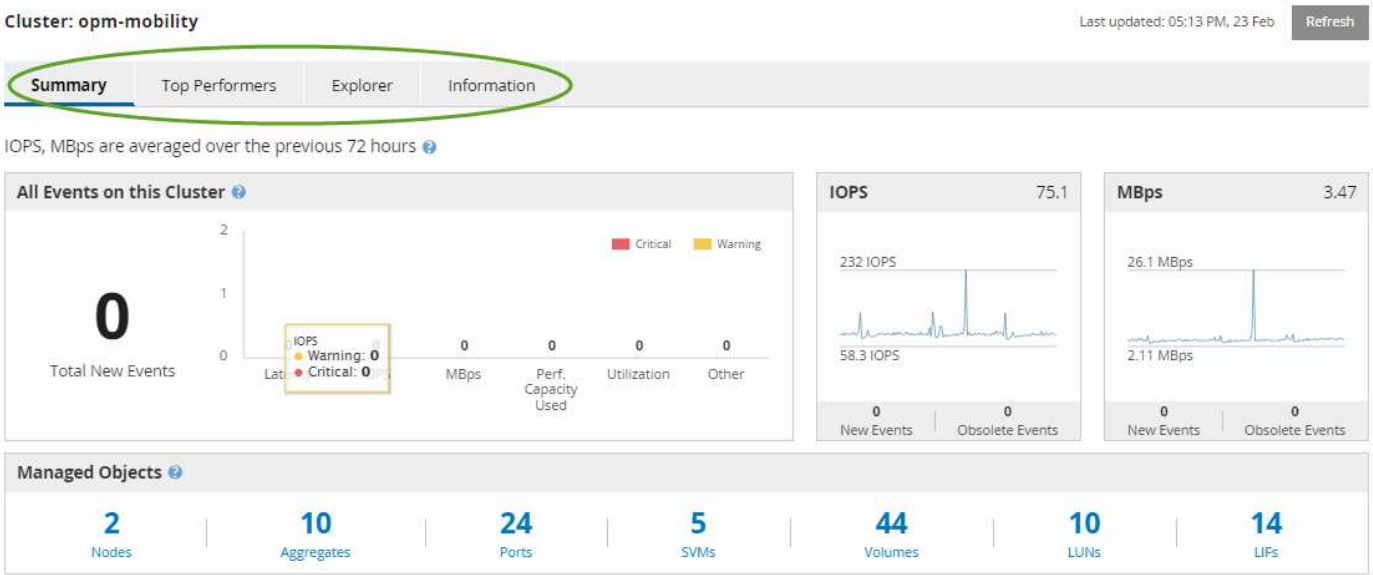
从 **Active IQ Unified Manager** 的 **Performance Cluster Landing** 页面监控集群性能

“性能群集登录”页面显示由 Unified Manager 实例监控的选定群集的高级性能状态。此页面使您能够评估特定群集的整体性能，并快速记录、定位或分配以解决所发现的任何特定于群集的事件。

了解 **Active IQ Unified Manager** 中的性能集群登录页面

性能集群登录页面提供所选集群的高级性能概述，重点介绍集群中前 10 个对象的性能状态。性能问题显示在页面顶部的“此集群上的所有事件”面板中。

性能集群登录页面提供了由 Unified Manager 实例管理的每个集群的高级概述。此页面为您提供有关事件和性能的信息，并使您能够监控集群并对其进行故障排除。下图显示了名为 opm-mobility 的集群的性能集群登录页面示例：



集群摘要页面上的事件计数可能与性能事件清单页面上的事件计数不匹配。这是因为当违反组合阈值策略时，集群摘要页面可以在延迟和利用率条中各显示一个事件，而性能事件清单页面在违反组合策略时仅显示一个事件。

如果群集已从 Unified Manager 管理中移除，则状态*已移除*将显示在页面顶端的群集名称的右

侧。

性能集群登录页面

在 **Active IQ Unified Manager** 中查看性能集群登录页面

“性能集群登录”页面显示选定集群的高级性能状态。通过该页面，您可以访问选定集群上存储对象的每个性能计数器的完整详细信息。

性能集群登录页面包括四个选项卡，将集群详细信息分为四个信息区域：

- 摘要页面
  - 集群事件窗格
  - MB/s 和 IOPS 性能图表
  - 受管对象窗格
- 最高性能页面
- 资源管理器页面
- 信息页面

性能集群摘要页面

查看 **Active IQ Unified Manager** 中的性能集群摘要页面

“性能集群摘要”页面提供了集群的活动事件、IOPS 性能和 MB/s 性能的摘要。此页面还包含集群中存储对象的总数。

在 **Active IQ Unified Manager** 中查看集群性能事件窗格

集群性能事件窗格显示集群的性能统计信息和所有活动事件。这在监控集群以及所有与集群相关的性能和事件时非常有用。

此集群窗格上的所有事件

此集群窗格上的所有事件显示前 72 小时的所有活动集群性能事件。活动事件总数显示在最左侧；此数字表示此集群中所有存储对象的所有新事件和已确认事件的总数。您可以单击活动事件总数链接以导航到事件清单页面，该页面经过筛选以显示这些事件。

集群的活动事件总数条形图显示活动关键事件和警告事件的总数：

- 延迟（节点、聚合、SVM、卷、LUN 和命名空间的总计）
- IOPS（集群、节点、聚合、SVM、卷、LUN 和命名空间的总计）
- MB/s（集群、节点、聚合、SVM、卷、LUN、命名空间、端口和 LIF 的总计）
- 已用性能容量（节点和聚合的总计）
- 利用率（节点、聚合和端口的总计）

- 其他（卷的缓存未命中率）

该列表包含由用户定义的阈值策略、系统定义的阈值策略和动态阈值触发的活动性能事件。

对于关键事件，图形数据（垂直计数器条）以红色（）显示，对于警告事件，以黄色（）显示。将光标悬停在每个垂直计数器条上，以查看事件的实际类型和数量。您可以单击 **Refresh** 以更新计数器面板数据。

您可以通过单击图例中的*关键*和*警告*图标，在总活动事件性能图表中显示或隐藏关键事件和警告事件。如果隐藏某些事件类型，图例图标将以灰色显示。

计数器面板

计数器面板显示前 72 小时的集群活动和性能事件，并包括以下计数器：

- **IOPS** 计数器面板

  IOPS 表示集群的运行速度，以每秒的输入/输出操作数表示。此计数器面板提供前 72 小时内集群 IOPS 运行状况的高级概述。您可以将光标放在图形趋势线上，以查看特定时间的 IOPS 值。

- **MB/s** 计数器面板

  MB/s 表示进出集群的数据量，以 MB/秒 为单位。此计数器面板提供前 72 小时内集群 MB/s 运行状况的高级概述。您可以将光标悬停在图形趋势线上，以查看特定时间的 MB/s 值。

灰色条中图表右上角的数字是过去 72 小时内的平均值。趋势线图底部和顶部显示的数字是过去 72 小时内的最小值和最大值。图表下方的灰色条包含过去 72 小时内的活动（新事件和已确认事件）和过时事件的计数。

计数器面板包含两种类型的事件：

- 活动

  指示性能事件当前处于活动状态（新建或已确认）。导致事件的问题尚未自行更正或尚未解决。存储对象的性能计数器仍高于性能阈值。

- 已废弃

  指示该事件不再处于活动状态。导致该事件的问题已自行更正或已解决。存储对象的性能计数器不再高于性能阈值。

对于*活动事件*，如果有一个事件，您可以将光标悬停在事件图标上，然后单击事件编号以链接到相应的事件详细信息页面。如果存在多个事件，则可以单击*查看所有事件*以显示事件清单页面，该页面经过筛选以显示所选对象计数器类型的所有事件。

查看 **Active IQ Unified Manager** 中的托管对象窗格

“性能摘要”选项卡中的“托管对象”窗格提供了集群的存储对象类型和计数的顶级概述。通过此窗格，您可以跟踪每个集群中对象的状态。

托管对象计数是截至上一个收集周期的时间点数据。每 15 分钟发现一次新对象。

单击任何对象类型的链接编号将显示该对象类型的对象性能清单页面。对象清单页面经过筛选，仅显示此集群上的对象。

托管对象包括：

- 节点

  集群中的物理系统。

- 聚合

  一组多个独立磁盘冗余阵列（RAID）组，可作为一个单位进行保护和调配管理。

- 端口

  节点上用于连接到网络上其他设备的物理连接点。

- 存储 **VM**

  通过唯一网络地址提供网络访问的虚拟机。SVM 可以从不同的命名空间提供数据，并且可以与集群的其他部分分开管理。

- 卷

  通过一个或多个受支持的访问协议保存可访问用户数据的逻辑实体。该计数包括 FlexVol 卷和 FlexGroup 卷；它不包括 FlexGroup 成分卷。

- **LUN**

  光纤通道 (FC) 逻辑单元或 iSCSI 逻辑单元的标识符。逻辑单元通常对应于存储卷，并在计算机操作系统中表示为设备。

- 网络接口

  表示到节点的网络接入点的逻辑网络接口。计数包括所有接口类型。

在 **Active IQ Unified Manager** 中查看性能最佳者页面

Top Performers 页面根据您选择的性能计数器显示性能最高或性能最低的存储对象。例如，在 Storage VM 类别中，您可以显示具有最高 IOPS、最高延迟或最低 MB/s 的 SVM。此页面还显示是否有任何最高性能对象具有任何活动的性能事件（新建或已确认）。

“最佳执行者”页面显示每个对象最多 10 个。请注意，Volume 对象包括 FlexVol 卷和 FlexGroup 卷。

- 时间范围

  您可以选择查看表现最佳者的时间范围；选定的时间范围适用于所有存储对象。可用时间范围：

  - 过去 1 小时
  - 过去 24 小时
  - 最近 72 小时（默认）
  - 过去 7 天

- 指标

单击 **Metric** 菜单选择其他计数器。计数器选项因对象类型而异。例如，**Volumes** 对象的可用计数器为 **Latency**、**IOPS** 和 **MB/s**。更改计数器会根据所选计数器重新加载面板数据，以显示表现最佳的项。

可用计数器：

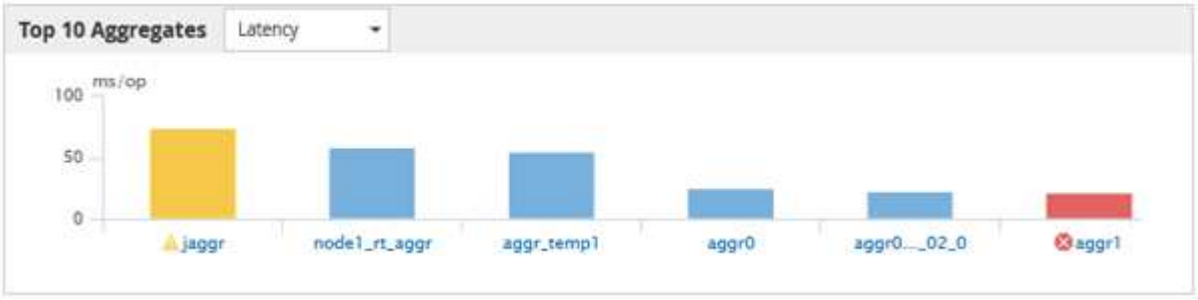
- 延迟
- IOPS
- MB/秒
- 已用性能容量（用于节点和聚合）
- 利用率（用于节点和聚合）

- 排序

单击*排序*菜单为所选对象和计数器选择升序或降序排序。选项为*从高到低*和*从低到高*。这些选项可用于查看性能最高或性能最低的对象。

- 计数器栏

图形中的计数器栏显示每个对象的性能统计信息，表示为该项目的条形图。条形图采用颜色编码。如果计数器未超出性能阈值，则计数器栏显示为蓝色。如果阈值违规处于活动状态（新的或已确认的事件），条形图将以事件的颜色显示：警告事件显示为黄色（ ），严重事件显示为红色（ ）。警告和严重事件的严重程度事件指示器图标会进一步指示阈值违规。



对于每个图形，X 轴显示选定对象类型的最高性能对象。Y 轴显示适用于选定计数器的单位。单击每个垂直条形图元素下方的对象名称链接，导航到选定对象的性能登录页面。

- 严重程度事件指示器

严重性事件 指示器图标显示在对象名称的左侧，用于最佳性能图表中的活动严重（ ）或警告（ ）事件。单击 严重性事件 指示器图标以查看：

- 一个事件

  导航到该事件的“事件详细信息”页面。

- 两个或两个以上的事件

  导航到“事件清单”页面，该页面经过筛选以显示选定对象的所有事件。

- 导出按钮

创建包含计数器栏中显示的数据的 `.csv`文件。您可以选择为正在查看的单个集群或数据中心中的所有集群

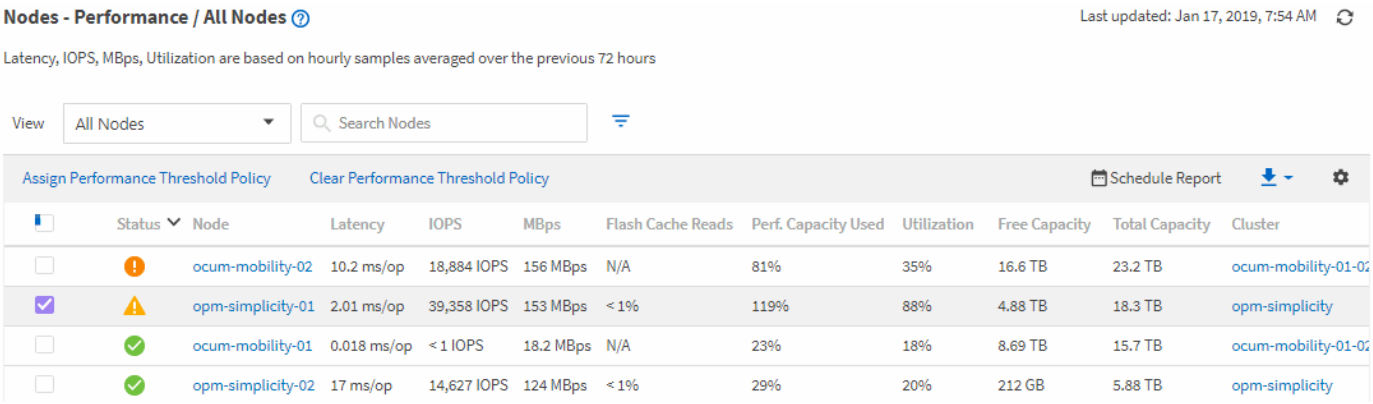
创建文件。

使用性能清单页面监控性能

使用 **Active IQ Unified Manager** 中的性能清单页面监控对象性能

对象清单性能页面显示对象类型类别中所有对象的性能信息、性能事件和对象健康状况。这使您可以一目了然地了解集群中每个对象的性能状态，例如，所有节点或所有卷的性能状态。

对象清单性能页面提供对象状态的高级概述，使您能够评估所有对象的整体性能并比较对象性能数据。您可以通过搜索、排序和筛选来细化对象清单页面的内容。这在监控和管理对象性能时很有用，因为它使您能够快速定位存在性能问题的对象并开始故障排除过程。



默认情况下，性能清单页面上的对象会根据对象性能关键程度进行排序。首先列出具有新的关键性能事件的对象，其次列出具有警告事件的对象。这为必须解决的问题提供了即时的可视化指示。所有性能数据均基于 72 小时的平均值。

您可以通过单击对象名称列中的对象名称，轻松地从对象清单性能页面导航至对象详细信息页面。例如，在 Performance/All Nodes 清单页面上，您可以单击 **Nodes** 列中的节点对象。对象详细信息页面提供有关所选对象的深入信息和详细内容，包括活动事件的并排比较。

查看 **Active IQ Unified Manager** 中所有存储对象的性能清单页面

使用性能清单页面可查看每个可用存储对象（如集群、聚合、卷等）的性能信息摘要。您可以链接到性能对象详细信息页面，以查看特定对象的详细信息。

默认情况下，视图页面中的对象会根据事件关键程度进行排序。首先列出具有严重事件的对象，其次列出具有警告事件的对象。这为必须解决的问题提供了即时的可视化指示。

您可以使用 报告 按钮将数据从这些页面导出为逗号分隔值（`.csv`）文件、Microsoft Excel 文件（`.xlsx`）或（`.pdf`）文档，然后使用导出的数据生成报告。此外，您可以自定义页面，然后使用 计划报告 按钮计划定期创建报告并通过电子邮件发送。

这些页面上的所有字段都可以在自定义视图和报告中使用。某些字段链接到相关页面，从而提供更详细的视图。

性能：所有集群视图

“性能：所有群集”视图显示由 Unified Manager 实例监控的每个群集的性能事件、数据和配置信息的概述。通过此页面，您可以监控群集的性能，并对性能问题和阈值事件进行故障排除。

您可以使用*分配性能阈值策略*和*清除性能阈值策略*按钮将性能阈值策略分配给对象清单页面上的任何对象，或从中清除阈值策略。

下面是“性能：所有群集”视图中的一些重要字段。

- 群集 FQDN：群集的完全限定域名（FQDN）。
- IOPS：集群上的每秒输入/输出操作。
- MB/s：集群上的吞吐量，以 MiB/秒为单位。
- 容量字段：可用容量和总容量（以 GiB 为单位）。
- 主机名或 IP 地址：集群管理 LIF 的主机名或 IP 地址（IPv4 或 IPv6）。
- 操作系统版本：集群上安装的 ONTAP 软件的版本。

> 如果在集群中的节点上安装了不同版本的 ONTAP 软件，则会列出最低的版本号。您可以从性能：所有节点视图中查看每个节点上安装的 ONTAP 版本。

- 阈值策略：在此存储对象上处于活动状态的用户定义的性能阈值策略。您可以将光标放在包含省略号（……）的策略名称上，以查看完整的策略名称或分配的策略名称列表。“分配性能阈值策略”和“清除性能阈值策略”按钮将保持禁用状态，直到您通过单击最左侧的复选框选择一个或多个对象。

性能：所有卷视图

“性能：所有卷”视图显示由 Unified Manager 实例监视的每个 FlexVol 卷和 FlexGroup 卷的性能事件、计数器数据和配置信息的概述。这使您能够快速监控卷的性能，并对性能问题和阈值事件进行故障排除。

如果要分析特定对象的延迟和吞吐量，请单击更多选项按钮 ⋮ ，然后单击 分析工作负载，您可以在工作负载分析页面上查看性能和容量图表。如果您具有 System Manager 的有效凭据，则可以在 System Manager 上查看详细信息。

> 对于数据保护（DP）卷，仅显示用户生成的流量的计数器值。此页面上不显示根卷。

下面是“性能：所有卷”视图中的一些重要字段。

- 样式：FlexVol 或 FlexGroup。
- 延迟：对于 FlexVol 卷，这是卷对所有 I/O 请求的平均响应时间，以每次操作的毫秒数为单位。对于 FlexGroup 卷，这是所有成分卷的平均延迟。
- IOPS/TB：基于工作负载正在消耗的总空间，每秒处理的输入/输出操作数，以 TB 为单位。此计数器衡量给定存储容量可以提供多少性能。
- IOPS：对于 FlexVol 卷，这是卷每秒的输入/输出操作数。对于 FlexGroup 卷，这是所有组成卷的 IOPS 之和。
- MB/s：对于 FlexVol 卷，这是以 MB/秒表示的卷吞吐量。对于 FlexGroup 卷，这是所有组成卷的 MB/s 之和。

- 容量字段：可用容量和总容量（以 GiB 为单位）。

有关详细信息，请参见以下链接：

- "为存储对象分配性能阈值策略"
- "从存储对象中删除性能阈值策略"
- "由 Unified Manager 监控的工作负载类型"
- "查看应用于特定卷或 LUN 的 QoS 策略组设置"
- "了解将数据分层到云的 Unified Manager 建议"
- "查看性能图表以比较同一 QoS 策略组中的 volume 或 LUN"

性能：所有聚合视图

“性能：所有聚合”视图显示由 Unified Manager 实例监控的每个聚合的性能事件、数据和配置信息的概述。此页面使您能够监控聚合的性能，并对性能问题和阈值事件进行故障排除。

下面是 Performance: All Aggregates 视图中的一些重要字段。

- 类型：聚合的类型：
  - HDD
  - 混合。结合硬盘和固态硬盘，但未启用 Flash Pool。
  - 混合（Flash Pool）。结合了硬盘和固态硬盘，并且已启用 Flash Pool。
  - SSD
  - SSD（FabricPool）。将 SSD 和云层相结合
  - HDD（FabricPool）。将 HDD 和云层相结合
  - VMDisk (SDS)。虚拟机中的虚拟磁盘
  - VMDisk（FabricPool）。结合虚拟磁盘和云层
  - LUN
- 非活动数据报告：是否在此聚合上启用或禁用非活动数据报告功能。启用后，此聚合上的卷会在“性能：所有卷”视图中显示冷数据量。当 ONTAP 版本不支持非活动数据报告时，此字段中的值为 "N/A"。
- 阈值策略：在此存储对象上处于活动状态的用户定义的性能阈值策略。可以将光标放在包含省略号（……）的策略名称上，以查看完整的策略名称或分配的策略名称列表。“分配性能阈值策略”和“清除性能阈值策略”按钮保持禁用状态，直到您通过单击最左侧的复选框选择一个或多个对象。有关详细信息，请参见以下链接：
- "为存储对象分配性能阈值策略"
- "从存储对象中删除性能阈值策略"

性能：所有节点视图

“性能：所有节点”视图显示了由 Unified Manager 实例监视的每个节点的性能事件、数据和配置信息的概述。这使您能够快速监控节点的性能，并对性能问题和阈值事件进行故障排除。

Flash Cache Reads 返回节点上由缓存满足而不是从磁盘返回的读取操作的百分比。仅针对节点显示 Flash Cache 数据，并且仅当节点中安装了 Flash Cache 模块时才会显示。

在*报告*菜单中，当 Unified Manager 及其管理的群集安装在没有外部网络连接的站点时，会提供*硬件清单报告*选项。此按钮生成一个 .csv 文件，其中包含完整的群集和节点信息列表；例如硬件型号和序列号、磁盘类型和计数、已安装的许可证等。此报告功能有助于在未连接到 NetApp Active IQ 平台的安全站点内续签合同。您可以使用*分配性能阈值策略*和*清除性能阈值策略*按钮，将性能阈值策略分配给对象清单页面上的任何对象，或从中清除阈值策略。

有关详细信息，请参见以下链接：

- "为存储对象分配性能阈值策略"
- "从存储对象中删除性能阈值策略"
- "生成硬件清单报告以续订合同"

性能：所有 **Storage VM** 视图

“性能：所有 Storage VM”视图显示由 Unified Manager 实例监控的每个存储虚拟机（SVM）的性能事件、数据和配置信息的概述。这使您能够快速监控 SVM 的性能，并对性能问题和阈值事件进行故障排除。此页面上的“延迟”字段报告所有 I/O 请求的平均响应时间，以每个操作的毫秒数为单位。

此页面上列出的 SVM 仅包括数据和集群 SVM。Unified Manager 不使用或显示管理或节点 SVM。

有关详细信息，请参见以下链接：

- "为存储对象分配性能阈值策略"
- "从存储对象中删除性能阈值策略"

性能：所有 **LUN** 视图

“性能：所有 LUN”视图显示了由 Unified Manager 实例监视的每个 LUN 的性能事件、数据和配置信息的概述。这使您能够快速监控 LUN 的性能，并对性能问题和阈值事件进行故障排除。

如果要分析特定对象的延迟和吞吐量，请单击更多图标 ⋮，然后单击*分析工作负载*，即可在*工作负载分析*页面上查看性能和容量图表。

有关详细信息，请参见以下链接：

- "监视一致性组关系中的 LUN"
- "配置 LUN"
- "为存储对象分配性能阈值策略"
- "从存储对象中删除性能阈值策略"
- "查看同一 QoS 策略组中的卷或 LUN"。
- "查看应用于特定卷或 LUN 的 QoS 策略组设置"
- "使用 API 调配 LUN"

性能：所有 **NVMe** 命名空间视图

“性能：所有 NVMe 命名空间”视图显示由 Unified Manager 实例监视的每个 NVMe 命名空间的性能事件、数据

和配置信息的概述。这使您能够快速监控命名空间的性能和运行状况，并对问题和阈值事件进行故障排除。

报告了以下信息（其中包括）：命名空间的当前状态。* 离线 - 不允许对命名空间进行读取或写入访问。* 在线 - 允许对命名空间进行读写访问。* NVFail - 由于 NVRAM 故障，命名空间自动脱机。* 空间错误 - 命名空间的空间已用尽。

有关详细信息，请参见以下链接：

- "为存储对象分配性能阈值策略"
- "从存储对象中删除性能阈值策略"

性能：所有网络接口视图

“性能：所有网络接口”视图显示由此 Unified Manager 实例监视的每个网络接口（LIF）的性能事件、数据和配置信息的概述。此页面使您能够快速监控接口的性能，并对性能问题和阈值事件进行故障排除。下面是“性能：所有网络接口”视图中的一些重要字段。

- IOPS：每秒的输入/输出操作。IOPS 不适用于 NFS LIF 和 CIFS LIF，并且对于这些类型显示为 N/A。
- 延迟：所有 I/O 请求的平均响应时间，以每次操作的毫秒数为单位。延迟不适用于 NFS LIF 和 CIFS LIF，并且对于这些类型显示为 N/A。
- 归属位置：接口的归属位置，显示为节点名称和端口名称，用冒号（:）分隔。如果位置以省略号（……）显示，则可以将光标悬停在位置名称上以查看完整位置。
- 当前位置：接口的当前位置，显示为节点名称和端口名称，用冒号（:）分隔。如果位置以省略号（……）显示，则可以将光标放在位置名称上以查看完整位置。
- 角色：接口角色：数据、集群、节点管理或集群间。

此页面上列出的接口包括数据 LIF、集群 LIF、节点管理 LIF 和集群间 LIF。Unified Manager 不使用或显示系统 LIF。

性能：所有端口视图

“性能：所有端口”视图显示由 Unified Manager 实例监视的每个端口的性能事件、数据和配置信息的概述。这使您能够快速监控端口的性能，并对性能问题和阈值事件进行故障排除。对于端口角色，将显示网络端口功能，即数据或集群。FCP 端口不能有角色，角色显示为 N/A。

性能计数器值仅针对物理端口显示。计数器值不针对 VLAN 或接口组显示。

有关详细信息，请参见以下链接：

- "为存储对象分配性能阈值策略"
- "从存储对象中删除性能阈值策略"

性能：**QoS** 策略组视图

QoS 策略组视图显示 Unified Manager 正在监视的群集上可用的 QoS 策略组。这包括传统 QoS 策略、自适应 QoS 策略以及使用性能服务级别分配的 QoS 策略。

以下是“性能：QoS 策略组”视图中的一些重要字段。

- QoS Policy Group：QoS 策略组的名称。对于已导入 Unified Manager 9.7 或更高版本的 NetApp Service Level Manager （NSLM） 1.3 策略，此处显示的名称包含 SVM 名称及其他信息，而这些信息在 NSLM 中定义 Performance Service Level 时并不包含在名称中。例如，名称 "NSLM_vs6_Performance_2_0" 表示这是在 SVM "vs6" 上创建的 NSLM 系统定义的 "Performance" PSL 策略，预期延迟为 "2 ms/op"。
- SVM：服务质量（QoS）策略组所属的存储虚拟机（SVM）。您可以单击存储虚拟机名称以导航到该存储虚拟机的详细信息页面。请注意，如果已在 Admin 存储虚拟机上创建了 QoS 策略，则此字段为空，因为此存储虚拟机类型表示集群。
- 最小吞吐量：将保证策略组提供的最小吞吐量（以 IOPS 为单位）。对于自适应策略，这是根据分配的存储对象大小分配给卷或 LUN 的每 TB 的最低预期 IOPS。
- 最大吞吐量：策略组不得超过的吞吐量（以 IOPS 和/或 MB/s 为单位）。当此字段为空时，这意味着在 ONTAP 中定义的最大吞吐量是无限的。对于自适应策略，这是分配给卷或 LUN 的每 TB 的最大（峰值）可能 IOPS，基于分配的存储对象大小或使用的存储对象大小。
- 绝对最小 IOPS：对于自适应策略，这是在预期 IOPS 小于此值时用作覆盖的绝对最小 IOPS 值。
- 块大小：为 QoS 自适应策略指定的块大小。
- 最小分配：是否使用“已分配空间”或“已用空间”来确定最大吞吐量（峰值） IOPS。
- 预期延迟：存储输入/输出操作的预期平均延迟。
- 共享：对于传统 QoS 策略，策略组中定义的吞吐量值是否在多个对象之间共享。
- 关联对象：分配给 QoS 策略组的工作负载数。您可以单击 QoS 策略组名称旁边的展开按钮（ ），查看有关策略组的更多详细信息。
- 分配的容量：服务质量（QoS）策略组中的对象当前正在使用的空间量。
- 关联对象：分配给 QoS 策略组的工作负载数，分为卷和 LUN。您可以单击该数字以导航到提供有关所选卷或 LUN 的更多详细信息的页面。

有关详细信息，请参见 "使用 QoS 策略组信息管理性能" 下的主题。

优化性能清单页面内容

在 **Active IQ Unified Manager** 中优化性能清单页面内容

性能对象的清单页面包含可帮助您优化对象清单数据内容的工具，使您能够轻松便捷地查找特定数据。

性能对象清单页面中包含的信息可能非常广泛，通常会跨越多个页面。这种全面的数据非常适合监控、跟踪和提高性能；但是，定位特定数据需要使用工具，以便您能够快速定位要查找的数据。因此，性能对象清单页面包含用于搜索、排序和筛选的功能。此外，搜索和筛选可以协同工作，进一步缩小结果范围。

在 **Active IQ Unified Manager** 的对象清单性能页面上搜索

您可以在“对象清单性能”页面上搜索字符串。使用页面右上角的*搜索*字段，根据对象名称或策略名称快速查找数据。这使您能够快速定位特定对象及其关联数据，或快速定位策略并查看关联策略对象数据。

步骤

1. 根据您的搜索要求，请执行以下选项之一：

要找到这个……	键入此……
特定对象	将对象名称输入到 搜索 字段中，然后单击 搜索。将显示您搜索的对象及其相关数据。
用户定义的性能阈值策略	将全部或部分策略名称输入 搜索 字段，然后单击 搜索。将显示分配给您搜索的策略的对象。

对 **Active IQ Unified Manager** 中"对象清单性能"页面上的数据进行排序

您可以按任意列以升序或降序对对象清单性能页面上的所有数据进行排序。这使您能够快速找到对象清单数据，这在检查性能或开始故障排除过程时很有帮助。

所选用于排序的列由突出显示的列标题名称和名称右侧指示排序方向的箭头图标来表示。向上箭头表示升序；向下箭头表示降序。默认排序顺序是按*状态*（事件关键度）降序排列，最关键的性能事件列在前面。

步骤

1. 您可以单击列名称以按升序或降序切换列的排序顺序。

   对象清单性能页面内容将根据所选列按升序或降序排列。

在 **Active IQ Unified Manager** 中筛选对象清单性能页面上的数据

您可以筛选对象清单性能页面中的数据，以根据特定条件快速查找数据。您可以使用筛选功能来缩小对象清单性能页面的内容范围，仅显示您指定的结果。这提供了一种非常有效的方法，用于仅显示您感兴趣的性能数据。

您可以使用“过滤”面板根据您的首选项自定义网格视图。可用的过滤器选项基于在网格中查看的对象类型。如果当前已应用过滤器，则已应用过滤器的数量会显示在“过滤器”按钮的右侧。

支持三种类型的过滤器参数。

参数	验证
字符串（文本）	运算符是*包含*、以……开头、以……结尾*和*不包含。
数字	运算符包括*大于*、小于、在最后*和*之间。
枚举（文本）	运算符是 **is** 和 **is not**。

每个筛选器都需要 Column（列）、Operator（运算符）和 Value（值）字段；可用的筛选器反映当前页面上的可筛选列。您最多可以应用四个筛选器。筛选结果基于组合的筛选器参数。筛选结果适用于筛选搜索中的所有页面，而不仅仅是当前显示的页面。

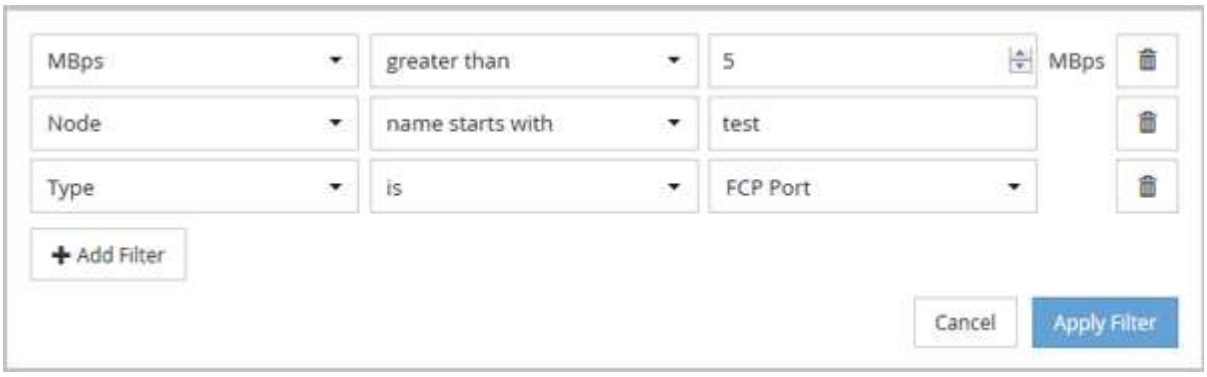
您可以使用“过滤”面板添加过滤器。

1. 在页面顶部，单击*筛选*按钮。此时将显示筛选面板。
2. 单击左侧下拉列表并选择一个对象；例如，*Cluster* 或性能计数器。
3. 单击中部下拉列表，然后选择要使用的运算符。
4. 在最后一个列表中，选择或输入一个值以完成此对象的筛选器。

5. 要添加其他过滤器，请单击 +添加过滤器。此时将显示一个额外的过滤器字段。使用前述步骤中描述的过程完成此过滤器。请注意，添加第四个过滤器后，+添加过滤器 按钮不再显示。
6. 单击*应用过滤器*。过滤器选项将应用于网格，过滤器的数量将显示在“过滤器”按钮的右侧。
7. 使用“筛选”面板，通过单击要删除的筛选器右侧的垃圾箱图标来删除单个筛选器。
8. 要删除所有过滤器，请点击过滤面板底部的*重置*。

筛选示例

该图显示了带有三个筛选条件的“筛选”面板。当您的筛选条件少于最多四个时，会显示 +添加筛选条件 按钮。



单击 应用过滤器 后，过滤面板将关闭，应用您的过滤器，并显示已应用的过滤器数量（ 3 ）。

查看 **Active IQ Unified Manager** 关于将数据分层到云的建议

“性能：所有卷”视图显示与存储在卷上的非活动（冷）用户数据大小相关的信息。在某些情况下，Unified Manager 会识别出通过将非活动数据分层到启用了 FabricPool 的聚合的云层（云提供商或 StorageGRID）而受益的某些卷。

FabricPool 在 ONTAP 9.2 中引入，因此，如果您使用的是 9.2 之前的 ONTAP 软件版本，则 Unified Manager 对数据分层的建议需要升级您的 ONTAP 软件。此外，ONTAP 9.4 中引入了 **`auto`** 分层策略，ONTAP 9.6 中引入了 **`all`** 分层策略，因此，如果建议使用自动分层策略，则必须升级到 ONTAP 9.4 或更高版本。

“性能：所有卷”视图上的以下三个字段提供了有关是否可以通过将非活动数据移动到云层来提高存储系统的磁盘利用率并节省性能层上的空间的信息。

- 分层策略

  分层策略确定卷上的数据是否仍保留在性能层上，或者某些数据是否从性能层移动到云层。

  此字段中的值指示在卷上设置的分层策略，即使卷当前不在 FabricPool 聚合上。分层策略仅在卷位于 FabricPool 聚合上时生效。

- 冷数据

  冷数据显示存储在卷上的非活动（冷）用户数据的大小。

  仅当使用 ONTAP 9.4 或更高版本的软件时，此处才会显示一个值，因为它要求部署该卷的聚合将

inactive data reporting parameter`设置为 `**enabled**，并且已达到最小冷却天数阈值（对于使用 **snapshot-only**`或 `**auto**`分层策略的卷）。否则，该值将列为"`N/A"。

- 云推荐

  在捕获了有关卷上的数据活动的足够信息后，Unified Manager 可能会确定不需要执行任何操作，或者可以通过将非活动数据分层到云层来节省性能层上的空间。

  Cold Data 字段每 15 分钟更新一次，但在卷上执行冷数据分析时，Cloud Recommendation 字段每 7 天更新一次。因此，冷数据的确切数量可能因字段而异。Cloud Recommendation 字段显示运行分析的日期。

启用"非活动数据报告"时，"冷数据"字段将显示非活动数据的确切数量。如果没有非活动数据报告功能，Unified Manager 将使用性能统计信息来确定卷上的数据是否处于非活动状态。在这种情况下，非活动数据的数量不会显示在"冷数据"字段中，但当您将光标悬停在单词 **Tier** 上以查看云建议时，它会显示出来。

您将看到的云推荐包括：

- 学习。未收集足够的数据以提供建议。
- 层。分析已确定该卷包含非活动（冷）数据，并且您应将该卷配置为将该数据移动到云层。在某些情况下，这可能需要您先将卷移动到启用了 FabricPool 的聚合。在其他情况下，如果卷已在 FabricPool 聚合中，则只需更改分层策略。
- 无操作。卷的非活动数据很少，卷已设置为 FabricPool 聚合上的 "auto" 分层策略，或者卷是数据保护卷。当卷处于脱机状态或正在 MetroCluster 配置中使用时，也会显示此值。

要移动卷，或更改卷分层策略或聚合非活动数据报告设置，请使用 ONTAP System Manager、ONTAP CLI 命令或这些工具的组合。

如果您使用应用程序管理员或存储管理员角色登录到 Unified Manager，当您将光标悬停在单词 **Tier** 上时，**Configure Volume** 链接在云建议中可用。单击此按钮可在 System Manager 中打开"卷"页面以进行建议的更改。

使用性能资源管理器页面监控性能

使用 **Active IQ Unified Manager** 中的 **Performance Explorer** 页面监控性能

"性能资源管理器"页面显示有关集群中每个对象性能的详细信息。该页面提供了所有集群对象性能的详细视图，使您能够选择和比较不同时间段内特定对象的性能数据。

您还可以评估所有对象的整体性能，并以并排格式比较对象性能数据。

在 **Active IQ Unified Manager** 中使用根对象进行性能监控

根对象是进行其他对象比较的基线。这使您能够查看来自其他对象的数据并将其与根对象进行比较，从而提供性能数据分析，帮助您排除故障并提高对象性能。

根对象名称显示在"比较"窗格的顶部。其他对象显示在根对象下方。虽然可以添加到"比较"窗格的其他对象的数量没有限制，但只允许使用一个根对象。根对象的数据会自动显示在"计数器图表"窗格的图形中。

无法更改根对象；它始终设置为正在查看的对象页面。例如，如果打开 Volume1 的 Volume Performance Explorer 页面，则 Volume1 是根对象，无法更改。如果要与其他根对象进行比较，则必须单击对象的链接并打开其登录页面。

仅为根对象显示事件和阈值。

筛选 **Active IQ Unified Manager** 网格中的相关对象

过滤使您可以在网格中显示更小、定义更明确的对象子集。例如，如果您在网格中有 25 个卷，则过滤使您可以仅查看吞吐量低于 90 MBps 或延迟大于 1 ms/op 的卷。

指定相关对象的时间范围

在 **Active IQ Unified Manager** 中指定相关对象的时间范围

“性能资源管理器”页面上的时间范围选择器使您能够指定对象数据比较的时间范围。指定时间范围可细化“性能资源管理器”页面的内容，以仅显示您指定的时间范围内的对象数据。

细化时间范围提供了一种仅显示您感兴趣的性能数据的有效方法。您可以选择预定义的时间范围或指定自定义时间范围。默认时间范围为前 72 小时。

在 **Active IQ Unified Manager** 中选择预定义的时间范围

选择预定义的时间范围是您在查看集群对象性能数据时自定义和聚焦数据输出的一种快速有效的方法。选择预定义的时间范围时，最多可提供 13 个月的数据。

步骤

1. 在*性能资源管理器*页面的右上角，单击*时间范围*。
2. 从*时间范围选择*面板的右侧，选择一个预定义的时间范围。
3. 单击*应用范围*。

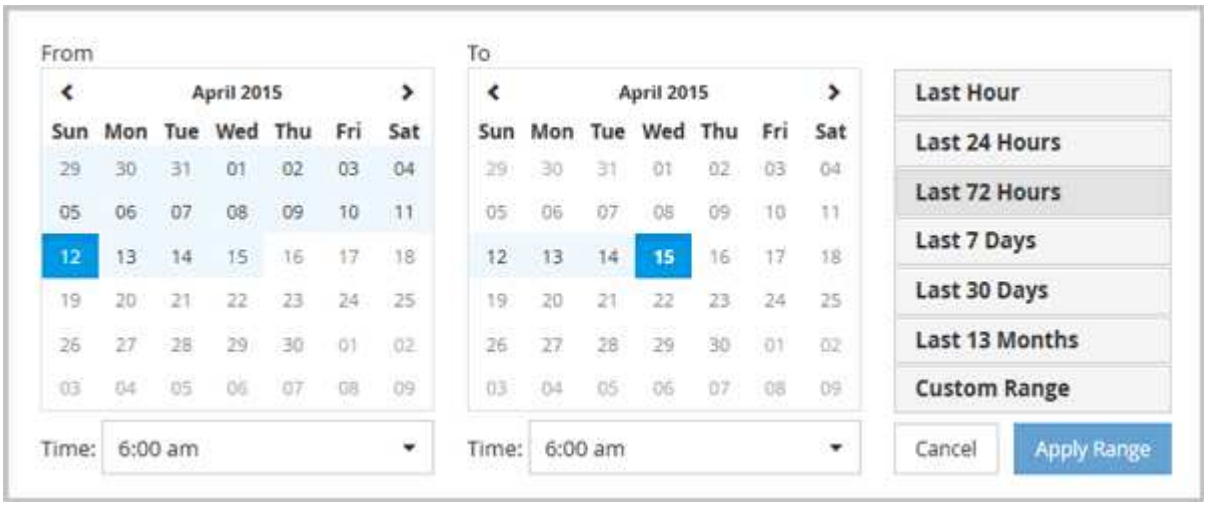
在 **Active IQ Unified Manager** 中指定自定义时间范围

通过“性能资源管理器”页面，您可以指定性能数据的日期和时间范围。在细化集群对象数据时，指定自定义时间范围比使用预定义时间范围具有更大的灵活性。

您可以选择介于 1 小时和 390 天之间的时间范围。13 个月等于 390 天，因为每个月都算作 30 天。指定日期和时间范围可提供更多详细信息，并使您能够放大特定性能事件或一系列事件。指定时间范围也有助于解决潜在的性能问题，因为指定日期和时间范围会更详细地显示围绕性能事件的数据。使用*时间范围*控件选择预定义的日期和时间范围，或指定最多 390 天的自定义日期和时间范围。预定义时间范围的按钮从*过去一小时*到*过去 13 个月*不等。

选择 过去 **13** 个月 选项或指定大于 30 天的自定义日期范围会显示一个对话框，提醒您显示大于 30 天的性能数据是使用每小时平均值而不是 5 分钟数据轮询绘制的。因此，可能会发生时间轴视觉粒度丢失。如果您单击对话框中的 不再显示 选项，则当您选择 过去 **13** 个月 选项或指定大于 30 天的自定义日期范围时，此消息不会显示。如果时间范围包括距今超过 30 天的时间/日期，则摘要数据也适用于较小的时间范围。

选择时间范围（自定义或预定义）时，30 天或更短的时间范围基于 5 分钟间隔数据样本。大于 30 天的时间范围基于一小时间隔数据样本。



1. 单击*时间范围*下拉框，随即显示时间范围面板。
2. 要选择预定义的时间范围，请单击 时间范围 面板右侧的 最后..... 按钮之一。选择预定义的时间范围时，最多可提供 13 个月的数据。所选的预定义时间范围按钮将突出显示，相应的日期和时间将显示在日历和时间选择器中。
3. 要选择自定义日期范围，请单击左侧 **From** 日历中的开始日期。单击 **<** or **>** 在日历中向前或向后导航。要指定结束日期，请单击右侧 **To** 日历中的日期。请注意，除非您指定其他结束日期，否则默认结束日期为今天。Time Range 面板右侧的 **Custom Range** 按钮会突出显示，表明您已选择自定义日期范围。
4. 要选择自定义时间范围，请点击 **From** 日历下方的 **Time** 控件，然后选择开始时间。要指定结束时间，请点击右侧 **To** 日历下方的 **Time** 控件，然后选择结束时间。时间范围面板右侧的 **Custom Range** 按钮会突出显示，表明您已选择自定义时间范围。
5. 您也可以在选择预定义的日期范围时指定开始和结束时间。如前所述选择预定义的日期范围，然后如前所述选择开始和结束时间。所选日期会在日历中突出显示，您指定的开始和结束时间会显示在*时间*控件中，而*自定义范围*按钮会突出显示。
6. 选择日期和时间范围后，单击*应用范围*。该时间范围的性能统计信息显示在图表和事件时间轴中。

在 **Active IQ Unified Manager** 中定义用于比较图形的相关对象

您可以在计数器图表窗格中定义用于数据和性能比较的相关对象列表。例如，如果您的存储虚拟机（SVM）遇到性能问题，则可以比较 SVM 中的所有卷，以确定可能导致问题的卷。

您可以将相关对象网格中的任何对象添加到比较窗格和计数器图表窗格中。这使您能够查看和比较多个对象的数据以及根对象的数据。您可以在相关对象网格中添加和移除对象；但是，比较窗格中的根对象不可移除。

将许多对象添加到“比较”窗格可能会对性能产生负面影响。要保持性能，您应该选择有限数量的图表进行数据比较。

步骤

1. 在对象网格中，找到要添加的对象，然后单击*添加*按钮。

   Add 按钮变为灰色，该对象将被添加到“比较”窗格中的附加对象列表中。对象的数据将被添加到“计数器图

表”窗格中的图形中。对象的眼睛图标（ ）的颜色与图形中对象的数据趋势线的颜色相匹配。

2. 可选： 隐藏或显示所选对象的数据：

要执行该操作.....	执行此操作.....
隐藏选定对象	在“比较”窗格中单击所选对象的眼睛图标（ ）。对象的数据将被隐藏，且该对象的眼睛图标变为灰色。
显示隐藏对象	单击“比较”窗格中选定对象的灰色眼睛图标。 眼睛图标恢复其原始颜色，对象数据将重新添加到“计数器图表”窗格的图形中。

3. 可选： 从*比较*窗格中删除所选对象：

要执行该操作.....	执行此操作.....
删除选定对象	将鼠标悬停在比较窗格中所选对象的名称上以显示删除对象按钮 (**X**)，然后单击该按钮。对象将从比较窗格中删除，其数据将从计数器图表中清除。
删除所有选定对象	单击比较窗格顶部的删除所有对象按钮（**X**）。所有选定对象及其数据都将被删除，只留下根对象。

了解 **Active IQ Unified Manager** 中的计数器图表

“计数器图表”窗格中的图表可用于查看和比较根对象以及从相关对象网格中添加的对象的性能数据。这可以帮助您了解性能趋势，并隔离和解决性能问题。

默认显示的计数器图表为事件、延迟、IOPS 和 MBps。您可以选择显示的可选图表是利用率、已使用性能容量、可用 IOPS、IOPS/TB 和缓存未命中率。此外，您可以选择查看延迟、IOPS、MBps 和已使用性能容量图表的总值或细分值。

默认情况下，性能资源管理器会显示某些计数器图表，无论存储对象是否全部支持这些图表。当不支持某个计数器时，计数器图表将为空，并显示消息 `Not applicable for <object>`。

图表显示根对象以及您在“比较”窗格中选择的所有对象的性能趋势。每个图表中的数据排列如下：

- **X**轴

  显示指定的时间段。如果未指定时间范围，则默认为前 72 小时。

- **Y** 轴

  显示选定对象特有的计数器单位。

趋势线颜色与“比较”窗格中显示的对象名称的颜色相匹配。您可以将光标定位在任何趋势线上的点上，以查看该点的时间和值的详细信息。

如果要调查图表中的特定时间段，可以使用下列方法之一：

- 使用 **<** 按钮展开计数器图表窗格，使其跨越页面宽度。
- 使用光标（切换到放大镜时）在图表中选择一部分时间范围来聚焦和放大该区域。您可以单击重置图表缩放，将图表返回到默认时间范围。
- 使用*缩放视图*按钮可显示包含扩展详细信息和阈值指标的大型单个计数器图表。

趋势线中偶尔会出现间隙。间隙意味着 Unified Manager 无法从存储系统收集性能数据，或者 Unified Manager 可能已停机。

了解 **Active IQ Unified Manager** 中的性能计数器图表类型

有标准性能图表显示选定存储对象的计数器值。每个细分计数器图表都会显示分为读取、写入和其他类别的总值。此外，当图表在缩放视图中显示时，一些细分计数器图表会显示更多详细信息。

下表显示了可用的性能计数器图表。

可用图表	图表说明
事件	显示与根对象的统计图表相关的关键、错误、警告和信息事件。除了性能事件之外，还会显示健康事件，以全面了解可能影响性能的原因。
延迟 - 总计	响应应用程序请求所需的毫秒数。请注意，平均延迟值是 I/O 加权的。
延迟 - 细分	与“延迟总计”中显示的信息相同，但性能数据分为读取、写入和其他延迟。此图表选项仅在所选对象为 SVM 、节点、聚合、卷、 LUN 或命名空间时适用。
延迟 - 集群组件	显示与“延迟总计”中相同的信息，但性能数据按集群组件划分为延迟。此图表选项仅在所选对象为卷时适用。
IOPS - 总计	每秒处理的输入/输出操作数。为节点显示时，选择 “Total” 将显示通过此节点移动的可能驻留在本地或远程节点上的数据的 IOPS，而选择 “Total (Local)” 将显示仅驻留在当前节点上的数据的 IOPS。
IOPS - 细分	与 IOPS 总计中显示的信息相同，但性能数据分为读取、写入和其他 IOPS。此图表选项仅适用于所选对象是 SVM、节点、聚合、卷、LUN 或命名空间时。 在缩放视图中显示时，如果在 ONTAP 中已配置，卷图表将显示 QoS 最小和最大吞吐量值。 为节点显示时，选择 “Breakdown” 将显示通过此节点移动的可能驻留在本地或远程节点上的数据的 IOPS 细分，而选择 “Breakdown (Local)” 将显示仅驻留在当前节点上的数据的 IOPS 细分。
IOPS - 协议	与 IOPS 总计中显示的信息相同，但性能数据分为 CIFS、NFS、FCP、NVMe 和 iSCSI 协议流量的单独图表。此图表选项仅在所选对象为 SVM 时适用。

可用图表	图表说明
IOPS/TB - 总计	基于工作负载正在消耗的总空间（以 TB 为单位）每秒处理的输入/输出操作数。此计数器也称为 I/O 密度，用于衡量给定存储容量可以提供多少性能。在缩放视图中显示时，如果在 ONTAP 中进行了配置，卷图表将显示 QoS 预期和峰值吞吐量值。 此图表选项仅在所选对象是卷时适用。
MB/秒 - 总计	每秒传输到对象和从对象传输的数据的兆字节数。
MB/秒 - 细分	与 MB/s 图表中显示的信息相同，但吞吐量数据分为磁盘读取、Flash Cache 读取、写入和其他。在缩放视图中显示时，如果在 ONTAP 中进行了配置，卷图表将显示 QoS 最大吞吐量值。 此图表选项仅在所选对象为 SVM、节点、聚合、卷、LUN 或命名空间时适用。 只有节点才会显示 Flash Cache 数据，并且仅当节点中安装了 Flash Cache 模块时才会显示这些数据。
已用性能容量 - 总计	节点或聚合正在消耗的性能容量的百分比。
已用性能容量 - 细分	已用性能容量数据分为用户协议和系统后台进程。此外，还显示了可用性能容量。
可用 IOPS - 总计	此对象上当前可用（空闲）的每秒输入/输出操作数。此数字是从 Unified Manager 计算出该对象可执行的总 IOPS 中减去当前已用 IOPS 的结果。此图表选项仅在所选对象为节点或聚合时适用。
利用率 - 总计	当前正在使用的对象的可用资源百分比。Utilization 表示节点的节点利用率、聚合的磁盘利用率和端口的带宽利用率。此图表选项仅在所选对象为节点、聚合或端口时适用。
缓存未命中率 - 总计	从磁盘而不是从缓存返回的客户端应用程序读取请求的百分比。此图表选项仅在所选对象为卷时适用。

选择要在 **Active IQ Unified Manager** 中显示的性能图表

“选择图表”下拉列表用于选择要在“计数器图表”窗格中显示的性能计数器图表类型。这使您能够根据性能要求查看特定数据和计数器。

步骤

1. 在*计数器图表*窗格中，单击*选择图表*下拉列表。
2. 添加或删除图表：

目的	操作
添加或删除单个图表	单击要显示或隐藏的图表旁边的复选框

目的	操作
添加所有图表	点击*全选*
删除所有图表	点击*取消全选*

您的图表选择会显示在计数器图表窗格中。请注意，添加图表时，新图表会插入到计数器图表窗格中，以匹配“选择图表”下拉列表中列出的图表顺序。选择其他图表可能需要额外滚动。

展开 **Active IQ Unified Manager** 中的计数器图表窗格

您可以展开计数器图表窗格，使图表更大，更易于阅读。

定义比较对象和计数器的时间范围后，您可以查看更大的计数器图表窗格。您可以使用 Performance Explorer 窗口中间的 **<** 按钮展开窗格。

步骤

1. 展开或缩小*计数器图表*窗格。

目的	操作
展开计数器图表窗格以适应页面的宽度	单击 **<** 按钮
将计数器图表窗格缩小到页面的右半部分	单击 **>** 按钮

在 **Active IQ Unified Manager** 中将计数器图表焦点更改为较短时间段

您可以使用鼠标缩小时间范围，以便在“计数器图表”窗格或“计数器图表缩放视图”窗口中专注于特定时间段。这使您能够看到性能数据、事件和阈值时间轴的任何部分的更精细和微观视图。

开始之前

光标必须已更改为放大镜，以指示此功能处于活动状态。

使用此功能时，这会更改时间轴以显示与更精细的显示相对应的值，时间范围 选择器上的时间和日期范围不会从图表的原始值发生更改。

步骤

1. 要放大到特定的时间段，请使用放大镜单击并拖动鼠标，以突出显示要详细查看的区域。

   所选时间段的计数器值填充计数器图表。

2. 要返回到*时间范围*选择器中设置的原始时间段，请单击*重置图表缩放*按钮。

   计数器图表以其原始状态显示。

在 **Active IQ Unified Manager** 事件时间线中查看事件详细信息

您可以在 Performance Explorer 的 Events Timeline 窗格中查看所有事件及其相关详细信息。这是一种快速有效地查看根对象在指定时间范围内发生的所有运行状况和性能事件的

方法，在排除性能问题时会有所帮助。

“事件时间线”窗格显示在选定时间范围内发生在根对象上的关键事件、错误事件、警告事件和信息事件。每个事件严重级别都有自己的时间线。单个和多个事件由时间线上的事件点表示。您可以将光标悬停在事件点上以查看事件详细信息。要增加多个事件的视觉粒度，您可以缩短时间范围。这会将多个事件分散为单个事件，使您能够分别查看和调查每个事件。

事件时间轴上的每个性能事件点与事件时间轴下方显示的计数器图表趋势线中的相应尖峰垂直对齐。这在事件和整体性能之间提供了直接的视觉相关性。健康事件也会显示在时间轴上，但这些类型的事件不一定与性能图表中的某个尖峰对齐。

步骤

1. 在*事件时间轴*窗格中，将光标悬停在时间轴上的事件点上，以查看该事件点上的事件摘要。

   弹出对话框显示有关事件类型、事件发生的日期和时间、状态和事件持续时间的信息。

2. 查看一个或多个事件的完整事件详细信息：

要执行该操作……	单击此处……
查看单个事件的详细信息	在弹出对话框中*查看事件详细信息*。
查看多个事件的详细信息	在弹出对话框中*查看事件详细信息*。 单击“多个事件”对话框上的单个事件将显示相应的事件详细信息页面。

计数器图表缩放视图

了解 **Active IQ Unified Manager** 中计数器图表的缩放视图

计数器图表提供了缩放视图，使您能够放大指定时间段内的性能详细信息。这使您能够以更高的粒度查看性能详细信息和事件，这在对性能问题进行故障排除时非常有用。

在缩放视图中显示时，某些细分图表提供的信息比图表不在缩放视图中时显示的信息更多。例如，IOPS 、IOPS/TB 和 MBps 细分图表缩放视图页面会显示卷和 LUN 的 QoS 策略值（如果在 ONTAP 中设置了这些值）。

对于系统定义的性能阈值策略，**Policies** 列表中仅提供“`Node resources over-utilized`”和“`QoS throughput limit breached`”策略。其他系统定义的阈值策略此时不可用。

在 **Active IQ Unified Manager** 中显示计数器图表缩放视图

计数器图表缩放视图为选定的计数器图表及其相关时间轴提供更精细的细节。这会放大计数器图表数据，使您能够更清晰地了解性能事件及其潜在原因。

您可以显示任何计数器图表的计数器图表缩放视图。

步骤

1. 单击 缩放视图 以在新的浏览器窗口中打开选定的图表。

2. 如果您正在查看细分图表，然后单击*缩放视图*，细分图表将显示在缩放视图中。如果您想更改视图选项，可以在缩放视图中选择*总计*。

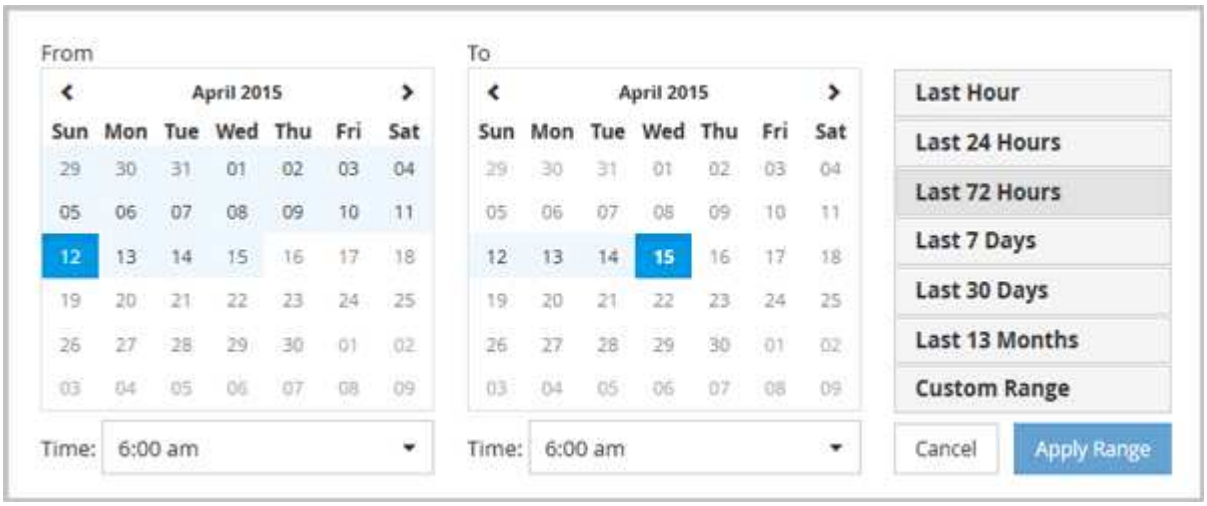
在 **Active IQ Unified Manager** 的缩放视图中指定时间范围

计数器图表缩放视图窗口中的*时间范围*控件使您能够为选定的图表指定日期和时间范围。这使您能够根据预设时间范围或您自己的自定义时间范围快速定位特定数据。

您可以选择介于 1 小时和 390 天之间的时间范围。13 个月等于 390 天，因为每个月都算作 30 天。指定日期和时间范围可提供更多详细信息，并使您能够放大特定性能事件或一系列事件。指定时间范围也有助于解决潜在的性能问题，因为指定日期和时间范围会更详细地显示围绕性能事件的数据。使用*时间范围*控件选择预定义的日期和时间范围，或指定最多 390 天的自定义日期和时间范围。预定义时间范围的按钮从*过去一小时*到*过去 13 个月*不等。

选择 过去 **13** 个月 选项或指定大于 30 天的自定义日期范围会显示一个对话框，提醒您显示大于 30 天的性能数据是使用每小时平均值而不是 5 分钟数据轮询绘制的。因此，可能会发生时间轴视觉粒度丢失。如果您单击对话框中的 不再显示 选项，则当您选择 过去 **13** 个月 选项或指定大于 30 天的自定义日期范围时，此消息不会显示。如果时间范围包括距今超过 30 天的时间/日期，则摘要数据也适用于较小的时间范围。

选择时间范围（自定义或预定义）时，30 天或更短的时间范围基于 5 分钟间隔数据样本。大于 30 天的时间范围基于一小时间隔数据样本。



1. 单击*时间范围*下拉框，随即显示时间范围面板。
2. 要选择预定义的时间范围，请单击 时间范围 面板右侧的 最后..... 按钮之一。选择预定义的时间范围时，最多可提供 13 个月的数据。所选的预定义时间范围按钮将突出显示，相应的日期和时间将显示在日历和时间选择器中。
3. 要选择自定义日期范围，请单击左侧 **From** 日历中的开始日期。单击 **<** or **>** 在日历中向前或向后导航。要指定结束日期，请单击右侧 **To** 日历中的日期。请注意，除非您指定其他结束日期，否则默认结束日期为今天。Time Range 面板右侧的 **Custom Range** 按钮会突出显示，表明您已选择自定义日期范围。
4. 要选择自定义时间范围，请点击 **From** 日历下方的 **Time** 控件，然后选择开始时间。要指定结束时间，请点击右侧 **To** 日历下方的 **Time** 控件，然后选择结束时间。时间范围面板右侧的 **Custom Range** 按钮会突出显示，表明您已选择自定义时间范围。
5. 您也可以在选择预定义的日期范围时指定开始和结束时间。如前所述选择预定义的日期范围，然后如前所述选择开始和结束时间。所选日期会在日历中突出显示，您指定的开始和结束时间会显示在*时间*控件中，而*自定义范围*按钮会突出显示。

6. 选择日期和时间范围后，单击*应用范围*。该时间范围的性能统计信息显示在图表和事件时间轴中。

在 **Active IQ Unified Manager** 的计数器图表缩放视图中选择性能阈值

在计数器图表缩放视图中应用阈值可提供性能阈值事件发生的详细视图。这使您能够应用或删除阈值，并立即查看结果，这在决定下一步是否应该进行故障排除时会有所帮助。

在计数器图表缩放视图中选择阈值可以查看有关性能阈值事件的精确数据。您可以应用计数器图表缩放视图 策略 区域下显示的任何阈值。

一次只能对计数器图表缩放视图中的对象应用一个策略。

步骤

1. 选择或取消选择与策略关联的 。

   所选阈值应用于计数器图表缩放视图。关键阈值显示为红线；警告阈值显示为黄线。

在 **Active IQ Unified Manager** 中按集群组件查看卷延迟

您可以使用“卷性能资源管理器”页面查看卷的详细延迟信息。Latency - Total 计数器图表显示卷上的总延迟，Latency - Breakdown 计数器图表可用于确定读取和写入延迟对卷的影响。

此外，“延迟-集群组件”图表显示了每个集群组件延迟的详细比较，以帮助确定每个组件如何影响卷上的总延迟。将显示以下集群组件：

- 网络
- 服务质量 (QoS) 上限
- 服务质量 (QoS) 下限
- 网络处理
- 集群互连
- 数据处理
- 聚合操作
- 卷激活
- MetroCluster 资源
- 云延迟
- 同步 SnapMirror

步骤

1. 在所选卷的*卷性能资源管理器*页面中，从延迟图表的下拉菜单中选择*集群组件*。

   此时将显示延迟 - 集群组件图表。

2. 要查看较大版本的图表，请选择*缩放视图*。

此时将显示集群组件对比图。您可以通过取消选择或选择与每个集群组件关联的 来限制比较。

3. 要查看具体值，请将光标移至图表区域以查看弹出窗口。

在 **Active IQ Unified Manager** 中按协议查看 **SVM IOPS** 流量

您可以使用性能/SVM 资源管理器页面查看 SVM 的详细 IOPS 信息。IOPS - 总计计数器图表显示 SVM 上的总 IOPS 使用情况，而 IOPS - 细分计数器图表可用于确定读取、写入和其他 IOPS 对 SVM 的影响。

此外，IOPS - 协议图表显示了 SVM 上正在使用的每个协议的 IOPS 流量的详细比较。以下协议可用：

- CIFS
- NFS
- FCP
- iSCSI
- NVMe-FC

步骤

1. 在您选择的 SVM 的 性能/**SVM** 资源管理器 页面中，从 IOPS 图表中，从下拉菜单中选择 协议。

   此时将显示 IOPS - 协议图表。

2. 要查看较大版本的图表，请选择*缩放视图*。

   显示 IOPS 高级协议比较图表。您可以通过取消选择或选择与协议关联的 来限制比较。

3. 要查看特定值，请将光标移动到任一图表的图表区域以查看弹出窗口。

查看卷和 **LUN** 延迟图表以验证 **Active IQ Unified Manager** 中的性能保证

您可以查看已订阅 “Performance Guarantee” 计划的卷和 LUN，以验证延迟未超过已保证的水平。

延迟性能保证是一个不应超过的每操作毫秒数值。它基于每小时平均值，而不是默认的五分钟性能收集周期。

步骤

1. 在*性能：所有卷*视图或*性能：所有 LUN*视图中，选择您感兴趣的卷或 LUN。
2. 在您选择的卷或 LUN 的*性能资源管理器*页面中，从*在中查看统计信息*选择器中选择*每小时平均值*。

   当五分钟采集的数据替换为每小时平均值时，延迟图表中的水平线将显示更平滑的线条。

3. 如果您在同一聚合中有属于性能保证的其他卷，则可以添加这些卷以在同一图表中查看其延迟值。

在 **Active IQ Unified Manager** 中查看所有 **SAN Array** 集群的性能

您可以使用性能：所有群集视图显示 All SAN Array 群集的性能状态。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

您可以在“性能：所有集群”视图中查看 All SAN Array 集群的概述信息，并在“集群/性能资源管理器”页面中查看详细信息。

步骤

1. 在左侧导航窗格中，单击 存储 > 集群。
2. 确保在 运行状况：所有集群 视图中显示 “Personality” 列，或使用 显示 / 隐藏 控件添加它。

   此列为您的 All SAN Array 集群显示 “All SAN Array”。
3. 要查看有关这些集群中性能的信息，请选择*性能：所有集群*视图。

   查看 All SAN Array 集群的性能信息。
4. 要查看有关这些集群性能的详细信息，请单击全 SAN 阵列集群的名称。
5. 单击*资源管理器*选项卡。
6. 在*集群/性能资源管理器*页面上，从*查看和比较*菜单中选择*此集群上的节点*。

   您可以比较此集群上两个节点的性能统计信息，以确保两个节点的负载几乎相同。如果两个节点之间存在较大差异，您可以将第二个节点添加到图表中，并在更长的时间范围内比较值，以识别任何配置问题。

在 **Active IQ Unified Manager** 中查看基于本地工作负载的节点 **IOPS**

节点 IOPS 计数器图表可以突出显示仅通过本地节点使用网络 LIF 对远程节点上的卷执行读/写操作的情况。IOPS - “Total (Local)” 和 “Breakdown (Local)” 图表显示仅驻留在当前节点上本地卷中的数据的 IOPS。

这些计数器图表的“`Local`”版本类似于性能容量和利用率的节点图表，因为它们也仅显示驻留在本地卷上的数据的统计信息。

通过将这些计数器图表的 “Local” 版本与这些计数器图表的常规总版本进行比较，您可以查看是否有大量流量通过本地节点访问远程节点上的卷。如果有太多操作通过本地节点到达远程节点上的卷，这种情况可能会导致性能问题，这可能表现为节点上的高利用率。在这些情况下，您可能需要将卷移动到本地节点，或者在远程节点上创建 LIF，以便连接来自访问该卷的主机的流量。

步骤

1. 在您所选节点的*性能/节点资源管理器*页面中，从 IOPS 图表中，从下拉菜单中选择*总计*。

   此时将显示 IOPS - 总计图表。
2. 单击 缩放视图，在新的浏览器选项卡中显示较大版本的图表。
3. 返回*性能/节点资源管理器*页面，在 IOPS 图表中，从下拉菜单中选择*总计（本地）*。

   此时将显示 IOPS - 总计（本地）图表。
4. 单击 缩放视图，在新的浏览器选项卡中显示较大版本的图表。

5. 查看彼此相邻的两个图表，并确定 IOPS 值似乎完全不同的区域。
6. 将光标移动到这些区域上，以比较特定时间点的本地 IOPS 和总 IOPS。

对象登录页的组件

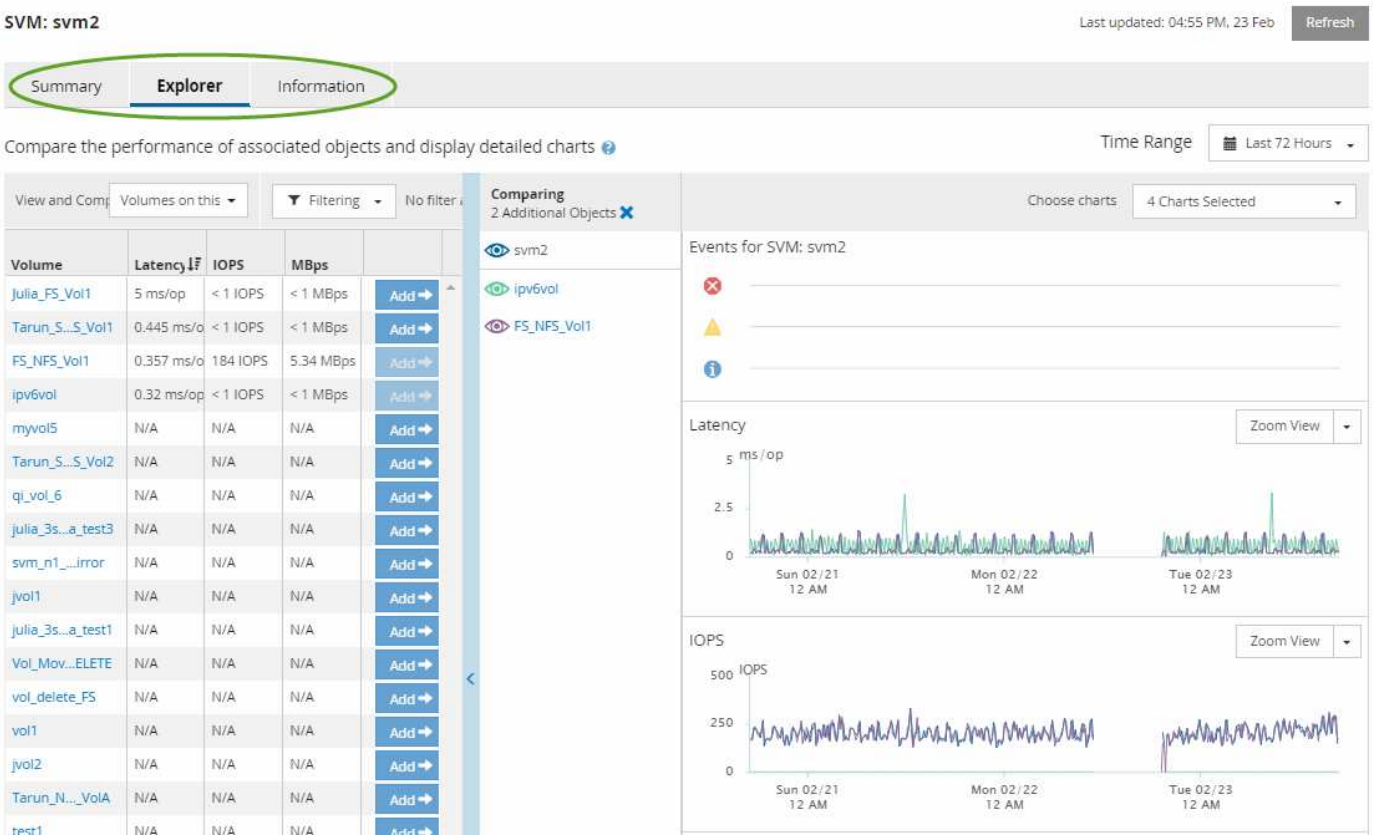
查看 **Active IQ Unified Manager** 中对象登录页面的组成部分

对象登录页面提供有关所有关键、警告和信息事件的详细信息。它们提供了所有集群对象性能的详细视图，使您能够选择和比较不同时间段内的单个对象。

通过“对象登录”页面，您可以检查所有对象的整体性能，并以并排格式比较对象性能数据。这在评估性能和排除事件故障时非常有用。

计数器摘要面板和计数器图表中显示的数据基于五分钟的采样间隔。页面左侧的对象清单网格中显示的数据基于一小时的采样间隔。

下图显示了显示资源管理器信息的对象登录页面的示例：



根据正在查看的存储对象，“对象登录”页面可以具有以下选项卡，这些选项卡提供有关对象的性能数据：

- 摘要

  显示三个或四个计数器图表，其中包含前 72 小时期间每个对象的事件和性能，包括显示该期间高值和低值的趋势线。

- 资源管理器

显示与当前对象相关的存储对象的网格，使您能够将当前对象的性能值与相关对象的性能值进行比较。此选项卡包括最多十一个计数器图表和一个时间范围选择器，使您能够执行各种比较。

- 信息

  显示有关存储对象的非性能配置属性的值，包括安装的 ONTAP 软件版本、HA 配对节点名称以及端口和 LIF 的数量。

- 性能最佳的对象

  对于群集：根据所选性能计数器显示性能最高或性能最低的存储对象。

- 故障转移规划

  对于节点：如果节点的 HA 伙伴发生故障，则显示对节点性能影响的估计。

- 详细信息

  对于卷：显示选定卷工作负载的所有 I/O 活动和操作的详细性能统计信息。此选项卡适用于 FlexVol 卷、FlexGroup 卷以及 FlexGroups 的组成部分。

在 **Active IQ Unified Manager** 中查看性能摘要页面

摘要页面显示计数器图表，其中包含有关前 72 小时内每个对象的事件和性能的详细信息。此数据不会自动刷新，但截至最后一次页面加载时是最新的。摘要页面中的图表回答了问题 我需要进一步查看吗?

图表和计数器统计

摘要图表提供了过去 72 小时内的快速、高级别概述，并帮助您识别需要进一步调查的可能问题。

摘要页面的计数器统计信息以图形方式显示。

您可以将光标悬停在图表中的趋势线上，以查看特定时间点的计数器值。摘要图表还显示以下计数器在过去 72 小时内的活动严重和警告事件总数：

- 延迟

  所有 I/O 请求的平均响应时间；以每个操作的毫秒数为单位表示。

  为所有对象类型显示。

- **IOPS**

  平均运行速度；以每秒的输入/输出操作表示。

  为所有对象类型显示。

- **MB/s**

  平均吞吐量；以 MB/秒 表示。

为所有对象类型显示。

- 已用性能容量

  节点或聚合正在消耗的性能容量百分比。

  仅针对节点和聚合显示。

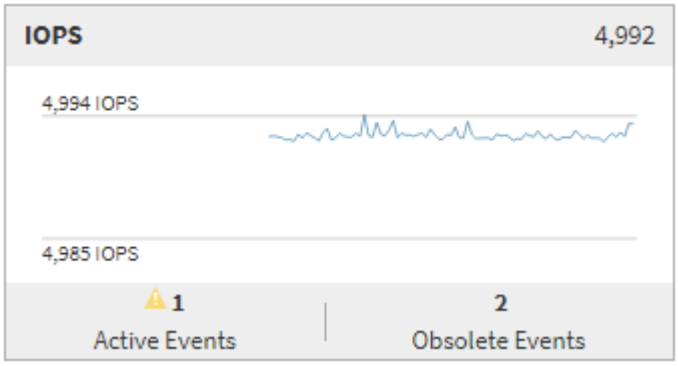
- 利用率

  节点和聚合的对象利用率或端口的带宽利用率百分比。

  仅针对节点、聚合和端口显示。

将光标悬停在活动事件的事件计数上，即可显示事件的类型和数量。严重事件显示为红色（ ），警告事件显示为黄色（ ）。

灰色条中图表右上角的数字是过去 72 小时内的平均值。趋势线图底部和顶部显示的数字是过去 72 小时内的最小值和最大值。图表下方的灰色条包含过去 72 小时内的活动（新事件和已确认事件）和过时事件的计数。



- 延迟计数器图表

  “延迟”计数器图表提供了前 72 小时内对象延迟的高级概述。延迟是指所有 I/O 请求的平均响应时间；以每次操作的毫秒数表示，即所考虑的集群存储组件中的数据包或块所经历的服务时间、等待时间或两者。

  Top （计数器值）： 标题中的数字显示前 72 小时内的平均值。

  中间（性能图）： 图表底部的数字显示最低延迟，图表顶部的数字显示前 72 小时内的最高延迟。将光标悬停在图表趋势线上，以查看特定时间的延迟值。

  底部（事件）：*悬停时，弹出窗口显示事件的详细信息。单击图表下方的 *活动事件 链接，导航到事件清单页面以查看完整的事件详细信息。

- **IOPS** 计数器图表

  IOPS 计数器图表提供了前 72 小时内对象 IOPS 运行状况的高级概述。IOPS 以每秒输入/输出操作的数量表示存储系统的速度。

  Top （计数器值）： 标题中的数字显示前 72 小时内的平均值。

  *中间（性能图表）：*图表底部的数字显示最低 IOPS，图表顶部的数字显示前 72 小时内的最高 IOPS。将光标置于图表趋势线上，可查看特定时间的 IOPS 值。

底部（事件）：*悬停时，弹出窗口显示事件的详细信息。单击图表下方的 *活动事件 链接，导航到事件清单页面以查看完整的事件详细信息。

- **MB/s** 计数器图表

  MB/s 计数器图表显示对象的 MB/s 性能，并指示与对象之间传输的数据量（以兆字节/秒为单位）。MB/s 计数器图表提供了前 72 小时内对象 MB/s 运行状况的高级概述。

  Top （计数器值）： 标题中的数字显示前 72 小时内的平均 MB/s 数。

  *中间（性能图）：*图表底部的值显示最低的 MB/s 数，图表顶部的值显示前 72 小时内的最高 MB/s 数。将光标悬停在图表趋势线上，以查看特定时间的 MB/s 值。

  底部（事件）：*悬停时，弹出窗口显示事件的详细信息。单击图表下方的 *活动事件 链接，导航到事件清单页面以查看完整的事件详细信息。

- 已用性能容量计数器图表

  Performance Capacity Used 计数器图表显示对象正在消耗的性能容量的百分比。

  Top（计数器值）： 标头中的数字显示前 72 小时内的平均已用性能容量。

  中间（性能图）： 图表底端的值显示最低已用性能容量百分比，图表顶端的值显示前 72 小时内的最高已用性能容量百分比。将光标悬停在图形趋势线上，以查看特定时间的已用性能容量值。

  底部（事件）：*悬停时，弹出窗口显示事件的详细信息。单击图表下方的 *活动事件 链接，导航到事件清单页面以查看完整的事件详细信息。

- 利用率计数器图表

  利用率计数器图表显示对象利用率百分比。利用率计数器图表提供了前 72 小时内对象或带宽利用率百分比的总体概述。

  *Top（计数器值）：*标题中的数字显示前 72 小时内的平均利用率百分比。

  *中间（性能图）：*图表底部的值显示最低利用率百分比，图表顶部的值显示前 72 小时内的最高利用率百分比。将光标悬停在图表趋势线上，以查看特定时间的利用率值。

  底部（事件）：*悬停时，弹出窗口显示事件的详细信息。单击图表下方的 *活动事件 链接，导航到事件清单页面以查看完整的事件详细信息。

事件

事件历史记录表（如适用）列出了该对象上发生的最新事件。单击事件名称会在“事件详细信息”页面上显示事件的详细信息。

查看 **Active IQ Unified Manager** 中的性能资源管理器页面

“性能资源管理器”页面使您能够比较集群中类似对象的性能，例如集群中的所有卷。这在对性能事件进行故障排除和微调对象性能时非常有用。您还可以将对象与根对象进行比较，根对象是进行其他对象比较的基准。

您可以单击 切换至运行状况视图 按钮以显示此对象的运行状况详细信息页面。在某些情况下，您可以了解有关此对象的存储配置设置的重要信息，这可能有助于进行故障排除。

“性能资源管理器”页面显示集群对象及其性能数据的列表。此页面以表格格式显示相同类型的所有集群对象（例如，卷及其特定对象的性能统计信息）。此视图提供集群对象性能的有效概览。

如果 “N/A” 出现在表的任何单元格中，则表示该计数器的值不可用，因为此时该对象上没有 I/O。

“性能资源管理器”页面包含以下组件：

- 时间范围

  使您能够为对象数据选择时间范围。

  您可以选择预定义范围，也可以指定自己的自定义时间范围。

- 查看和比较

  使您能够选择在网格中显示哪种类型的相关对象。

  可用的选项取决于根对象类型及其可用数据。您可以单击“查看和比较”下拉列表来选择对象类型。您选择的对象类型将显示在列表中。

- 筛选

  使您能够根据自己的偏好来缩小接收的数据量。

  您可以创建应用于对象数据的筛选器——例如，IOPS 大于 4。您最多可同时添加四个筛选条件。

- 比较

  显示您已选择与根对象进行比较的对象列表。

  “比较”窗格中对象的数据显示在计数器图表中。

- 查看统计信息

  对于卷和 LUN ，允许您选择是在每个收集周期（默认为 5 分钟）之后显示统计信息，还是将统计信息显示为每小时平均值。此功能使您能够查看延迟图表，以支持 NetApp “性能保证”计划。

- 计数器图表

  显示每个对象性能类别的图形化数据。

  通常，默认情况下只显示三到四个图表。选择图表组件使您可以显示其他图表，或隐藏特定的图表。您还可以选择显示或隐藏事件时间轴。

- 事件时间轴

  显示在时间范围组件中选择的时间轴上发生的性能和运行状况事件。

使用 QoS 策略组信息管理性能

使用 Active IQ Unified Manager 中的 QoS 策略组信息管理性能

Unified Manager 使您能够查看正在监视的所有集群上可用的服务质量（QoS）策略组。这些策略可能已使用 ONTAP 软件（System Manager 或 ONTAP CLI）或由 Unified Manager 性能服务级别策略定义。Unified Manager 还显示已分配 QoS 策略组的卷和 LUN。

有关调整 QoS 设置的详细信息，请参见 "性能管理概述"

使用 Active IQ Unified Manager 中的存储 QoS 控制工作负载吞吐量

您可以创建服务质量 (QoS) 策略组，以控制其包含的工作负载的每秒 I/O (IOPS) 或吞吐量 (MB/s) 限制。如果工作负载位于没有设置限制的策略组中，例如默认策略组，或者设置的限制不满足您的需求，则可以增加限制或将工作负载移动到具有所需限制的新策略组或现有策略组。

“传统” QoS 策略组可以分配给单个工作负载；例如，单个卷或 LUN。在这种情况下，工作负载可以使用完整的吞吐量限制。QoS 策略组也可以分配给多个工作负载；在这种情况下，吞吐量限制在工作负载之间“共享”。例如，为三个工作负载分配 9,000 IOPS 的 QoS 限制将限制组合 IOPS 不超过 9,000 IOPS。

“自适应” QoS 策略组也可以分配给单个工作负载或多个工作负载。但是，即使分配给多个工作负载，每个工作负载也会获得完整的吞吐量限制，而不是与其他工作负载共享吞吐量值。此外，自适应 QoS 策略会根据每个工作负载的卷大小自动调整吞吐量设置，从而在卷大小发生变化时保持 IOPS 与 TB 的比例。例如，如果在自适应 QoS 策略中将峰值设置为 5,000 IOPS/TB，则 10 TB 卷的吞吐量最大值为 50,000 IOPS。如果稍后将卷的大小调整为 20 TB，自适应 QoS 会将最大值调整为 100,000 IOPS。

从 ONTAP 9.5 开始，您可以在定义自适应 QoS 策略时包含块大小。这有效地将策略从 IOPS/TB 阈值转换为 MB/s 阈值，适用于工作负载使用非常大的块大小并最终占用大量吞吐量的情况。

对于共享组 QoS 策略，当策略组中所有工作负载的 IOPS 或 MB/s 超过设置的限制时，策略组会限制工作负载的活动，这可能会降低策略组中所有工作负载的性能。如果策略组限制生成了动态性能事件，则事件描述将显示相关策略组的名称。

在“性能：所有卷”视图中，您可以按 IOPS 和 MB/s 对受影响的卷进行排序，以查看哪些工作负载的使用率最高，从而可能导致了该事件。在“性能/卷资源管理器”页面中，您可以选择其他卷或该卷上的 LUN，以与受影响的工作负载的 IOPS 或 MBps 吞吐量使用情况进行比较。

通过将过度使用节点资源的工作负载分配给更严格的策略组设置，策略组将限制工作负载以限制其活动，这可以减少该节点上资源的使用。但是，如果希望工作负载能够使用更多的节点资源，则可以增加策略组的值。

您可以使用 System Manager、ONTAP 命令或 Unified Manager 性能服务级别来管理策略组，包括以下任务：

- 创建策略组
- 在策略组中添加或删除工作负载
- 在策略组之间移动工作负载
- 更改策略组的吞吐量限制

- 将工作负载移动到其他聚合和/或节点

查看 **Active IQ Unified Manager** 上所有集群中可用的 **QoS** 策略组

您可以显示 Unified Manager 正在监视的群集上可用的所有 QoS 策略组的列表。这包括传统 QoS 策略、自适应 QoS 策略以及由 Unified Manager 性能服务级别策略管理的 QoS 策略。

步骤

1. 在左侧导航窗格中，单击*存储* > **QoS** 策略组。

   默认显示性能：传统 QoS 策略组视图。

2. 查看每个可用传统 QoS 策略组的详细配置设置。
3. 单击 QoS 策略组名称旁边的展开按钮（ ）可查看有关策略组的更多详细信息。
4. 在视图菜单中，选择其中一个附加选项以查看所有自适应 QoS 策略组或查看使用 Unified Manager 性能服务级别创建的所有 QoS 策略组。

在 **Active IQ Unified Manager** 中查看同一 **QoS** 策略组中的卷或 **LUN**

您可以显示已分配给同一 QoS 策略组的卷和 LUN 的列表。

对于在多个卷之间“shared”的传统 QoS 策略组，这有助于查看某些卷是否过度使用为策略组定义的吞吐量。它还可以帮助您决定是否可以将其他卷添加到策略组，而不会对其他卷产生负面影响。

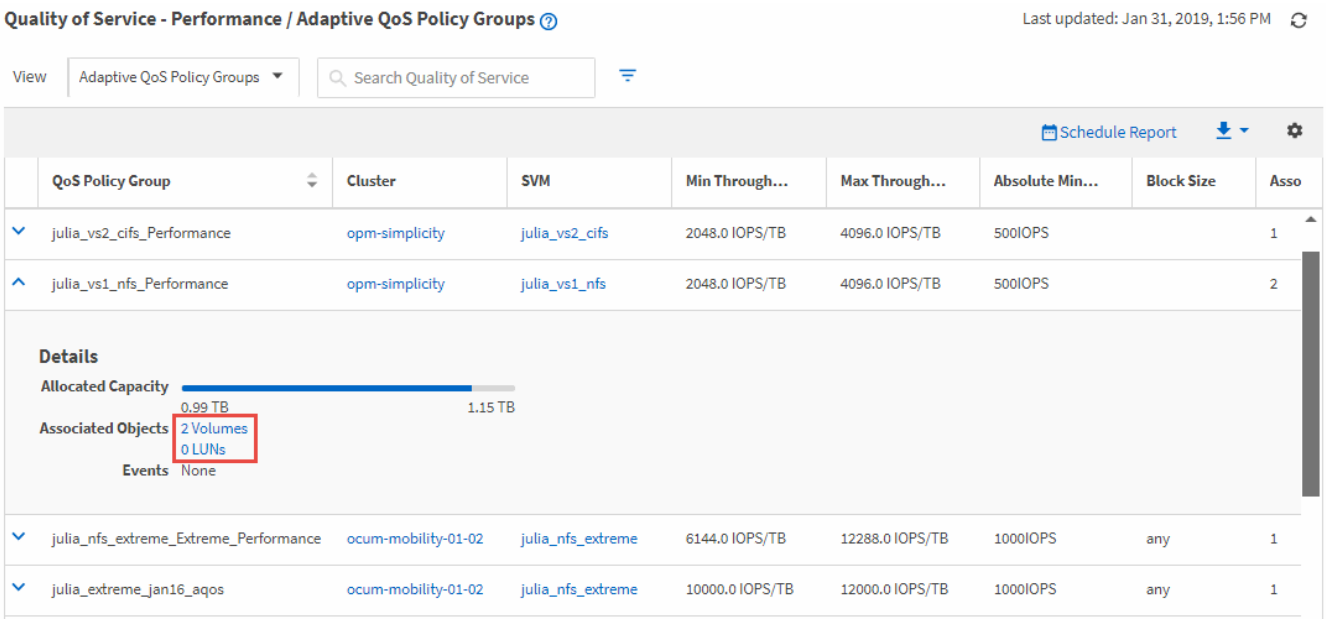
对于自适应 QoS 策略和 Unified Manager 性能服务级别策略，这有助于查看正在使用某个策略组的所有卷或 LUN，以便查看如果更改 QoS 策略的配置设置将影响哪些对象。

步骤

1. 在左侧导航窗格中，单击*存储* > **QoS** 策略组。

   默认显示性能：传统 QoS 策略组视图。

2. 如果您对传统策略组感兴趣，请留在此页面。否则，请选择其他视图选项之一，以显示所有自适应 QoS 策略组，或者由 Unified Manager 性能服务级别创建的所有 QoS 策略组。
3. 在您感兴趣的 QoS 策略中，单击 QoS 策略组名称旁边的展开按钮（ ）以查看更多详细信息。



4. 单击卷或 LUN 链接以查看使用此 QoS 策略的对象。

   此时将显示卷或 LUN 的性能清单页面，以及使用 QoS 策略的对象的排序列表。

在 **Active IQ Unified Manager** 中查看卷或 **LUN** 的 **QoS** 策略组设置

您可以查看已应用于卷和 LUN 的 QoS 策略组，也可以链接到性能/QoS 策略组视图以显示每个 QoS 策略的详细配置设置。

以下显示了查看应用于卷的 QoS 策略的步骤。查看 LUN 的此信息的步骤与此类似。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。

   默认情况下会显示运行状况：所有卷视图。

2. 在视图菜单中，选择*性能：QoS 策略组中的卷*。
3. 找到要查看的卷，然后向右滚动，直到看到 **QoS** 策略组 列。
4. 单击 QoS Policy Group 名称。

   相应的服务质量页面的显示取决于它是传统的 QoS 策略、自适应 QoS 策略还是使用 Unified Manager 性能服务级别创建的 QoS 策略。

5. 查看服务质量（QoS）策略组的详细配置设置。
6. 单击 QoS 策略组名称旁边的展开按钮（ ）可查看有关策略组的更多详细信息。

比较 **Active IQ Unified Manager** 中同一 **QoS** 策略组内的卷或 **LUN**

您可以查看相同 QoS 策略组中的卷和 LUN，然后在单个 IOPS、MB/s 或 IOPS/TB 图表上比较性能，以识别任何问题。

比较同一个 QoS 策略组中卷的性能的步骤如下所示。查看 LUN 此信息的步骤类似。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。

   默认情况下会显示运行状况：所有卷视图。

2. 在视图菜单中，选择*性能：QoS 策略组中的卷*。
3. 单击要查看的卷的名称。

   此时将显示该卷的“性能资源管理器”页面。

4. 在 View and Compare 菜单中，选择 **Volumes in same QoS Policy Group**。

   下表列出了共享相同 QoS 策略的其他卷。

5. 单击 添加 按钮将这些卷添加到图表中，以便您可以比较图表中所有选定卷的 IOPS、MB/s、IOPS/TB 和其他性能计数器。

   您可以更改时间范围，以查看不同时间间隔（而非默认的 72 小时）内的性能。

使用 **Active IQ Unified Manager** 查看吞吐量图表中的 **QoS** 策略

您可以在性能资源管理器和工作负载分析 IOPS、IOPS/TB 和 MB/s 图表中查看已应用于卷或 LUN 的 ONTAP 定义的服务质量（QoS）策略设置。图表中显示的信息因已应用于工作负载的 QoS 策略类型而异。

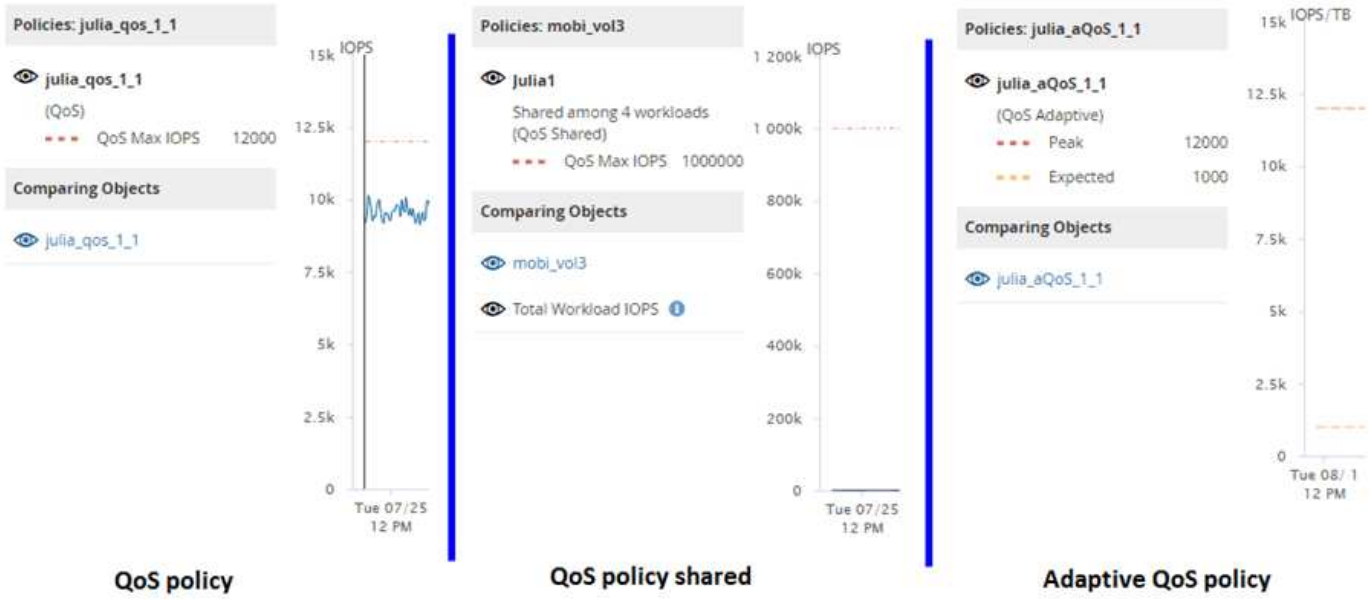
吞吐量最大值（或"`peak`"）设置定义了工作负载可以消耗的最大吞吐量，从而限制了对竞争系统资源的工作负载的影响。吞吐量最小值（或"`expected`"）设置定义了工作负载必须可用的最小吞吐量，以便无论竞争工作负载的需求如何，关键工作负载都能满足最小吞吐量目标。

用于 IOPS 和 MB/s 的共享和非共享 QoS 策略使用术语 “minimum” 和 “maximum” 来定义下限和上限。ONTAP 9.3 中引入的针对 IOPS/TB 的自适应 QoS 策略使用术语 “expected” 和 “peak” 来定义下限和上限。

虽然 ONTAP 可让您创建这两种类型的 QoS 策略，但根据它们应用于工作负载的方式，QoS 策略在性能图表中的显示方式有三种。

策略类型	功能	**Unified Manager** 界面中的指示器
分配给单个工作负载的 QoS 共享策略，或分配给单个或多个工作负载的 QoS 非共享策略	每个工作负载都可以消耗指定的吞吐量设置	显示 “(QoS)”
分配给多个工作负载的 QoS 共享策略	所有工作负载共享指定的吞吐量设置	显示“`(QoS Shared)`”
分配给单个工作负载或多个工作负载的自适应 QoS 策略	每个工作负载都可以消耗指定的吞吐量设置	显示“`(QoS Adaptive)`”

下图显示了计数器图表中如何显示三个选项的示例。



当已在 IOPS 中定义的普通 QoS 策略出现在工作负载的 IOPS/TB 图表中时，ONTAP 将 IOPS 值转换为 IOPS/TB 值，Unified Manager 在 IOPS/TB 图表中显示该策略以及文本 “在 IOPS 中定义的 QoS”。

当已在 IOPS/TB 中定义的自适应 QoS 策略出现在工作负载的 IOPS 图表中时，ONTAP 会将 IOPS/TB 值转换为 IOPS 值，Unified Manager 将在 IOPS 图表中显示该策略以及文本“`QoS Adaptive - Used, defined in IOPS/TB`”或“`QoS Adaptive - Allocated, defined in IOPS/TB`”，具体取决于峰值 IOPS 分配设置的配置方式。当分配设置设置为“`allocated-space`”时，系统将根据卷的大小计算峰值 IOPS。当分配设置设置为“`used-space`”时，系统将根据存储在卷中的数据量并考虑存储效率来计算峰值 IOPS。

仅当卷使用的逻辑容量大于或等于 128 GB 时，IOPS/TB 图表才会显示性能数据。在所选时间范围内，当已用容量低于 128 GB 时，图表中会显示间隙。

在 **Active IQ Unified Manager** 中查看工作负载 **QoS** 最小值和最大值设置

您可以在性能资源管理器图表中查看卷或 LUN 上的 ONTAP 定义的服务质量（Quality of Service，QoS）策略设置。吞吐量最大值设置限制了竞争工作负载对系统资源的影响。吞吐量最低设置可确保关键工作负载满足最低吞吐量目标，无论竞争工作负载的需求如何。

只有在 ONTAP 中配置了 QoS 吞吐量“`minimum`”和“`maximum`” IOPS 及 MB/s 设置时，这些设置才会显示在计数器图表中。吞吐量最低设置仅在运行 ONTAP 9.2 或更高版本软件的系统上可用，且仅在 AFF 系统上可用，目前只能为 IOPS 设置此项。

自适应 QoS 策略从 ONTAP 9.3 开始提供，使用 IOPS/TB 而非 IOPS 来表示。这些策略会根据卷大小自动调整每个工作负载的 QoS 策略值，从而在卷大小变化时保持 IOPS 与 TB 的比率。自适应 QoS 策略组只能应用于卷。QoS 术语 “expected”（预期）和 “peak”（峰值）用于自适应 QoS 策略，而非最小值和最大值。

当工作负载吞吐量在前一小时的每个性能收集期间超过定义的 QoS 最大策略设置时，Unified Manager 会生成 QoS 策略违规的警告事件。在每个收集期间，工作负载吞吐量可能仅在短时间内超过 QoS 阈值，但 Unified Manager 会在图表上显示收集期间的“`average`”吞吐量。因此，您可能会看到 QoS 事件，而工作负载的吞吐量可能未超过图表中显示的策略阈值。

步骤

1. 在您选择的卷或 LUN 的*性能资源管理器*页面中，执行以下操作以查看 QoS 上限和下限设置：

目的	操作
查看 IOPS 上限（QoS 最大值）	在 IOPS 总计或分解图表中，单击*缩放视图*。
查看 MB/s 上限（QoS 最大值）	在 MB/s 总计或明细图表中，单击*缩放视图*。
查看 IOPS 下限（QoS 最小值）	在 IOPS 总计或分解图表中，单击*缩放视图*。
查看 IOPS/TB 上限（QoS 峰值）	对于卷，在 IOPS/TB 图表中，单击*缩放视图*。
查看 IOPS/TB 下限（预期 QoS）	对于卷，在 IOPS/TB 图表中，单击*缩放视图*。

虚线水平线表示在 ONTAP 中设置的最大或最小吞吐量值。您还可以查看何时实施了对 QoS 值的更改。

2. 要查看与 QoS 设置相比的特定 IOPS 和 MB/s 值，请将光标移动到图表区域以查看弹出窗口。

如果您注意到某些卷或 LUN 具有非常高的 IOPS 或 MB/s 并且对系统资源造成压力，您可以使用 System Manager 或 ONTAP CLI 调整 QoS 设置，以便这些工作负载不会影响其他工作负载的性能。

有关调整 QoS 设置的详细信息，请参见 "性能管理概述"

使用性能容量和可用 IOPS 信息管理性能

在 Active IQ Unified Manager 中管理性能容量和可用 IOPS

Performance capacity 表示在不超过该资源的有用性能的情况下，可以从资源中获得多少吞吐量。使用现有性能计数器查看时，性能容量是在延迟成为问题之前从节点或聚合中获得最大利用率的点。

Unified Manager 从每个群集中的节点和聚合收集性能容量统计信息。_所用性能容量_是当前正在使用的性能容量的百分比，_空闲性能容量_是仍然可用的性能容量的百分比。

虽然可用性能容量提供了仍然可用的资源的一定百分比，但 可用 *IOPS* 会告诉您在达到最大性能容量之前可以添加到资源中的 IOPS 数量。通过使用此指标，您可以确保能够将具有预定 IOPS 数量的工作负载添加到资源中。

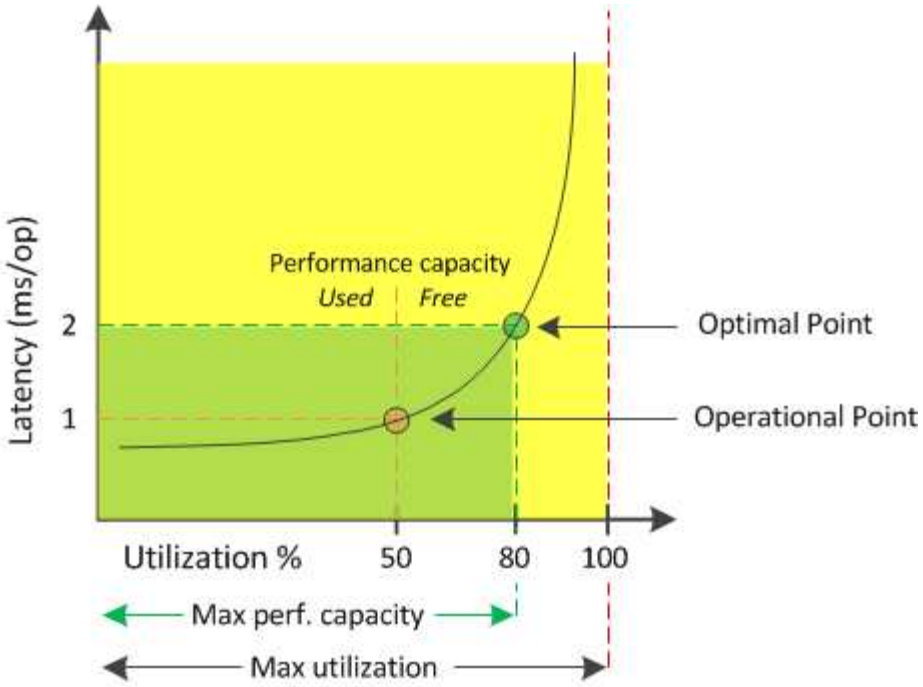
监控性能容量信息具有以下优势：

- 协助工作流调配和平衡。
- 帮助您防止节点过载或其资源超出最佳点，从而减少故障排除的需要。
- 帮助您更精确地确定可能需要额外存储设备的位置。

了解 Active IQ Unified Manager 中已用性能容量计数器

已用性能容量计数器可帮助您确定节点或聚合的性能是否已达到如果工作负载增加性能可能会下降的临界点。它还可以显示节点或聚合当前是否在特定时间段内被过度使用。已用性能容量类似于利用率，但前者提供了有关特定工作负载的物理资源中可用性能功能的更多见解。

最佳已用性能容量是指节点或聚合具有最佳利用率和延迟（响应时间）并得到高效利用的点。下图显示了聚合的延迟与利用率示例曲线。



在此示例中，*operational point* 标识聚合当前以 50% 的利用率运行，延迟为 1.0 ms/op。根据从聚合中捕获的统计数据，Unified Manager 确定此聚合还有额外的可用性能容量。在此示例中，*optimal point* 被标识为聚合处于 80% 利用率且延迟为 2.0 ms/op 的点。因此，您可以向此聚合添加更多卷和 LUN，以便更有效地使用您的系统。

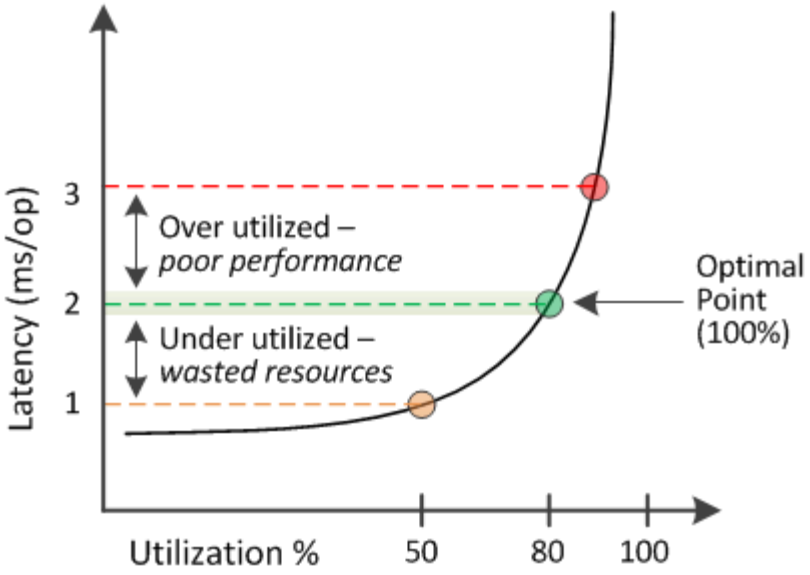
已用性能容量计数器预计会大于“`utilization`”计数器，因为性能容量将对延迟的影响计算在内。例如，如果节点或聚合的已用量为 70%，则性能容量值可能在 80% 到 100% 的范围内，具体取决于延迟值。

但是，在某些情况下，仪表板页面上的利用率计数器可能会更高。这是正常的，因为仪表板会在每个收集期间刷新当前计数器值；它不会像 Unified Manager 用户界面中的其他页面那样显示一段时间内的平均值。已用性能容量计数器最适合用作一段时间内平均性能的指标，而利用率计数器最适合用于确定资源的即时使用情况。

使用 **Active IQ Unified Manager** 中的已用性能容量值

此性能容量已用值可帮助您识别当前被过度利用或未充分利用的节点和聚合。这使您能够重新分配工作负载，以提高存储资源的效率。

下图显示了资源的延迟与利用率曲线，并使用彩色点标识了当前操作点可能位于的三个区域。



- 性能容量使用百分比等于 100 处于最佳点。

  目前，资源正在得到有效利用。

- 使用的性能容量百分比高于 100 表示节点或聚合过度使用，并且工作负载正在接收次优性能。

  不应向资源中添加新工作负载，并且可能需要重新分配现有工作负载。

- 使用的性能容量百分比低于 100 表示节点或聚合未充分利用，并且资源未得到有效利用。

  可以向资源中添加更多工作负载。

与利用率不同，性能容量使用百分比可以高于 100%。没有最高百分比，但资源在过度使用时通常在 110% 至 140% 的范围内。百分比越高，表示资源存在严重问题。

了解 **Active IQ Unified Manager** 中的可用 **IOPS**

可用 IOPS 计数器标识可在资源达到其限制之前添加到节点或聚合中的剩余 IOPS 数量。

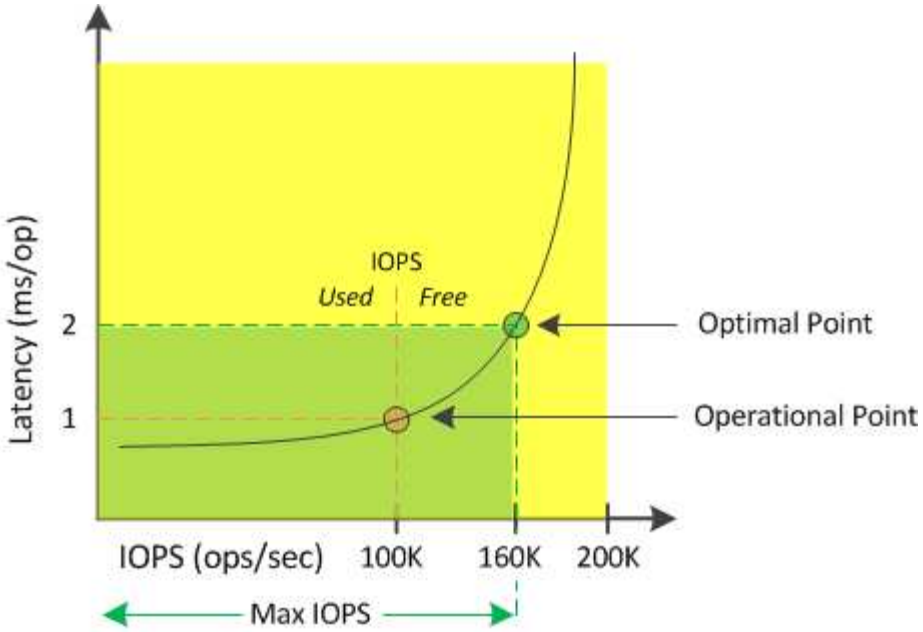
节点可提供的总 IOPS 取决于节点的物理特性，例如 CPU 数量、CPU 速度和 RAM 容量。聚合可提供的总 IOPS 基于磁盘的物理属性，例如 SATA、SAS 或 SSD 磁盘。

聚合中所有卷的总 IOPS 可能与聚合的总 IOPS 不匹配。以下知识库文章对此进行了讨论：KB "为什么聚合中所有卷 IOPs 的总和与聚合 IOPs 不匹配？"

虽然性能空闲容量计数器提供仍然可用的资源的百分比，但可用的 IOPS 计数器会告诉您在达到最大性能容量之前可以添加到资源中的 IOPS（工作负载）的确切数量。

例如，如果您使用的是一对 FAS2520 和 FAS8060 存储系统，则性能容量空闲值为 30% 意味着您有一些空闲性能容量。但是，该值并不能让您了解还可以向这些节点部署多少个工作负载。可用 IOPS 计数器可能显示 FAS8060 上有 500 个可用 IOPS，但 FAS2520 上只有 100 个可用 IOPS。

下图显示了节点的示例延迟与 IOPS 曲线。



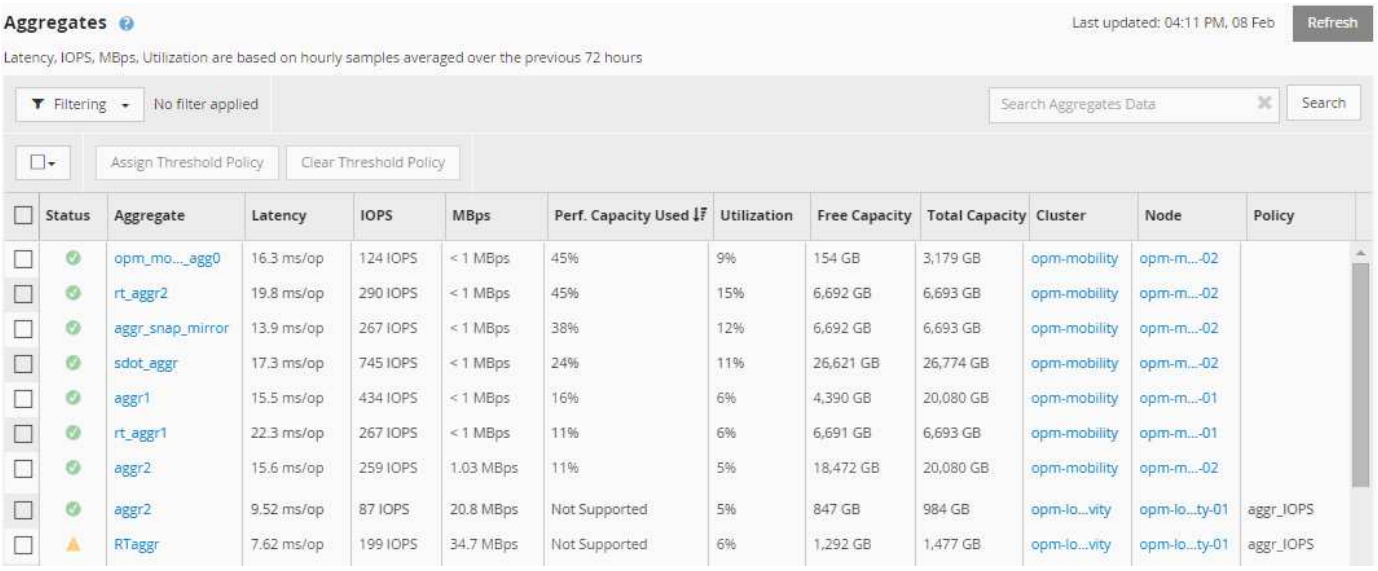
资源可以提供的最大 IOPS 数是性能容量使用计数器为 100%（最佳点）时的 IOPS 数。操作点标识节点当前以 100K IOPS 运行，延迟为 1.0 ms/op。根据从节点捕获的统计数据，Unified Manager 确定节点的最大 IOPS 为 160K，这意味着有 60K 空闲或可用 IOPS。因此，您可以向此节点添加更多工作负载，以便更有效地使用您的系统。

当资源中的用户活动极少时，可用 IOPS 值是假设基于每个 CPU 核心约 4,500 IOPS 的通用工作负载来计算的。这是因为 Unified Manager 缺乏准确估计所服务工作负载特征的数据。

在 **Active IQ Unified Manager** 中查看节点和聚合性能容量使用值

您可以监视集群中所有节点或所有聚合的性能容量使用值，也可以查看单个节点或聚合的详细信息。

“使用的性能容量”值显示在“仪表板”、“性能清单”页面、“最高性能对象”页面、“创建阈值策略”页面、“性能资源管理器”页面和详细信息图表中。例如，“性能：所有聚合”页面提供了一个“使用的性能容量”列，用于查看所有聚合的使用的性能容量值。



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

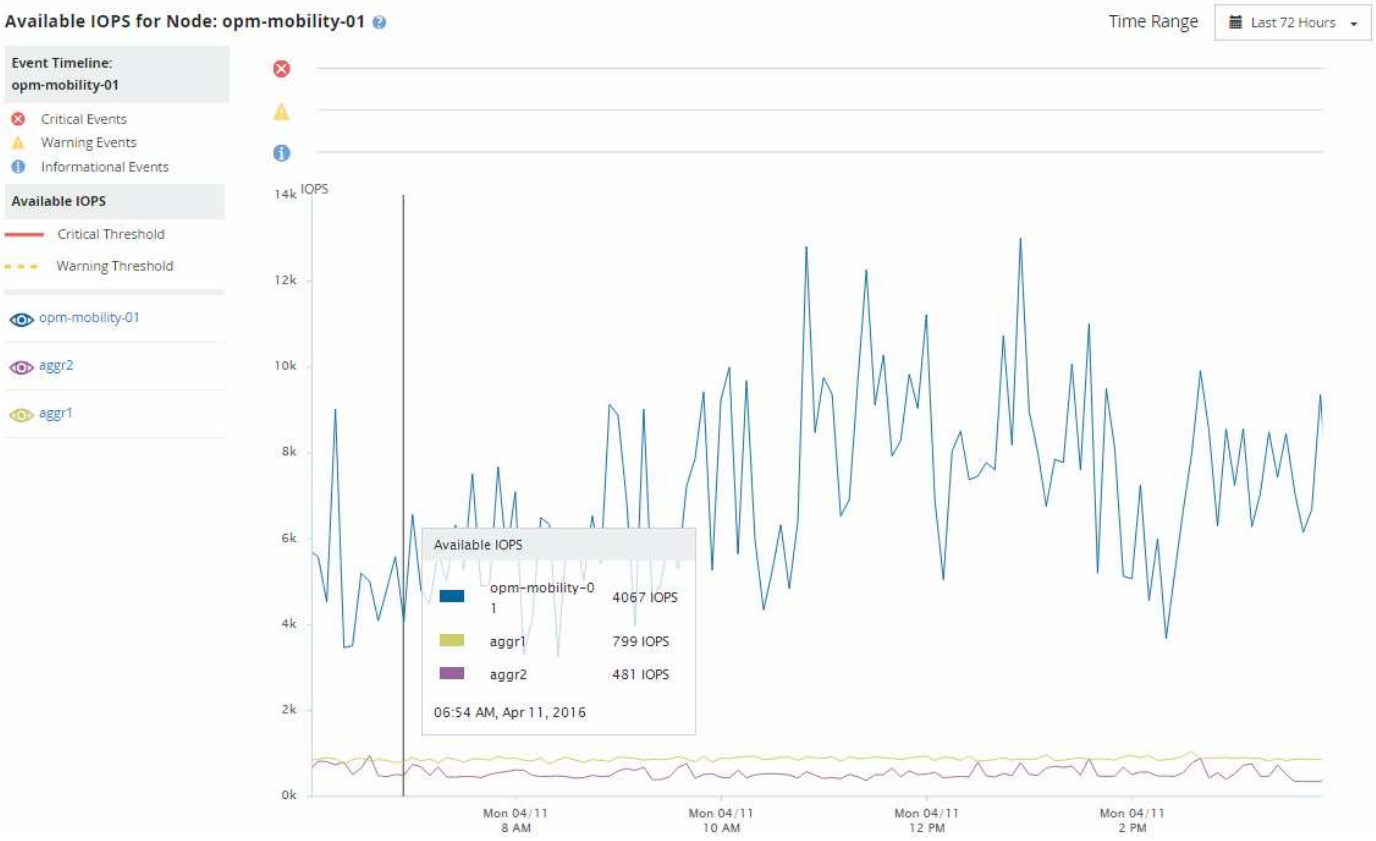
监控使用的性能容量计数器使您能够识别以下内容：

- 任何集群上的任何节点或聚合是否具有较高的已用性能容量值
- 是否任何集群上的任何节点或聚合具有活动的性能容量使用事件
- 集群中具有最高和最低性能容量已用值的节点和聚合
- 与具有高性能容量使用值的节点或聚合结合使用的延迟和利用率计数器值
- 如果其中一个节点发生故障，HA 对中节点的性能容量使用值将如何受到影响
- 具有高性能容量使用值的聚合上最繁忙的卷和 LUN

查看 **Active IQ Unified Manager** 中节点和聚合的可用 **IOPS** 值

您可以监控集群中所有节点或所有聚合的可用 IOPS 值，也可以查看单个节点或聚合的详细信息。

可用的 IOPS 值显示在“性能清单”页面以及节点和聚合的“性能资源管理器”页面图表中。例如，在“节点/性能资源管理器”页面中查看节点时，您可以从列表中选择 “可用 IOPS” 计数器图表，以便比较该节点以及该节点上多个聚合的可用 IOPS 值。



通过监控可用 IOPS 计数器，您可以识别：

- 具有最大可用 IOPS 值的节点或聚合，以帮助确定可以部署未来工作负载的位置。
- 可用 IOPS 值最小的节点或聚合，用于确定应监视以防将来可能出现性能问题的资源。
- 可用 IOPS 值较小的聚合中最繁忙的卷和 LUN。

在 **Active IQ Unified Manager** 中查看性能容量计数器图表

您可以在“性能资源管理器”页面上查看节点和聚合的性能容量使用图表。这使您能够查看特定时间范围内选定节点和聚合的详细性能容量数据。

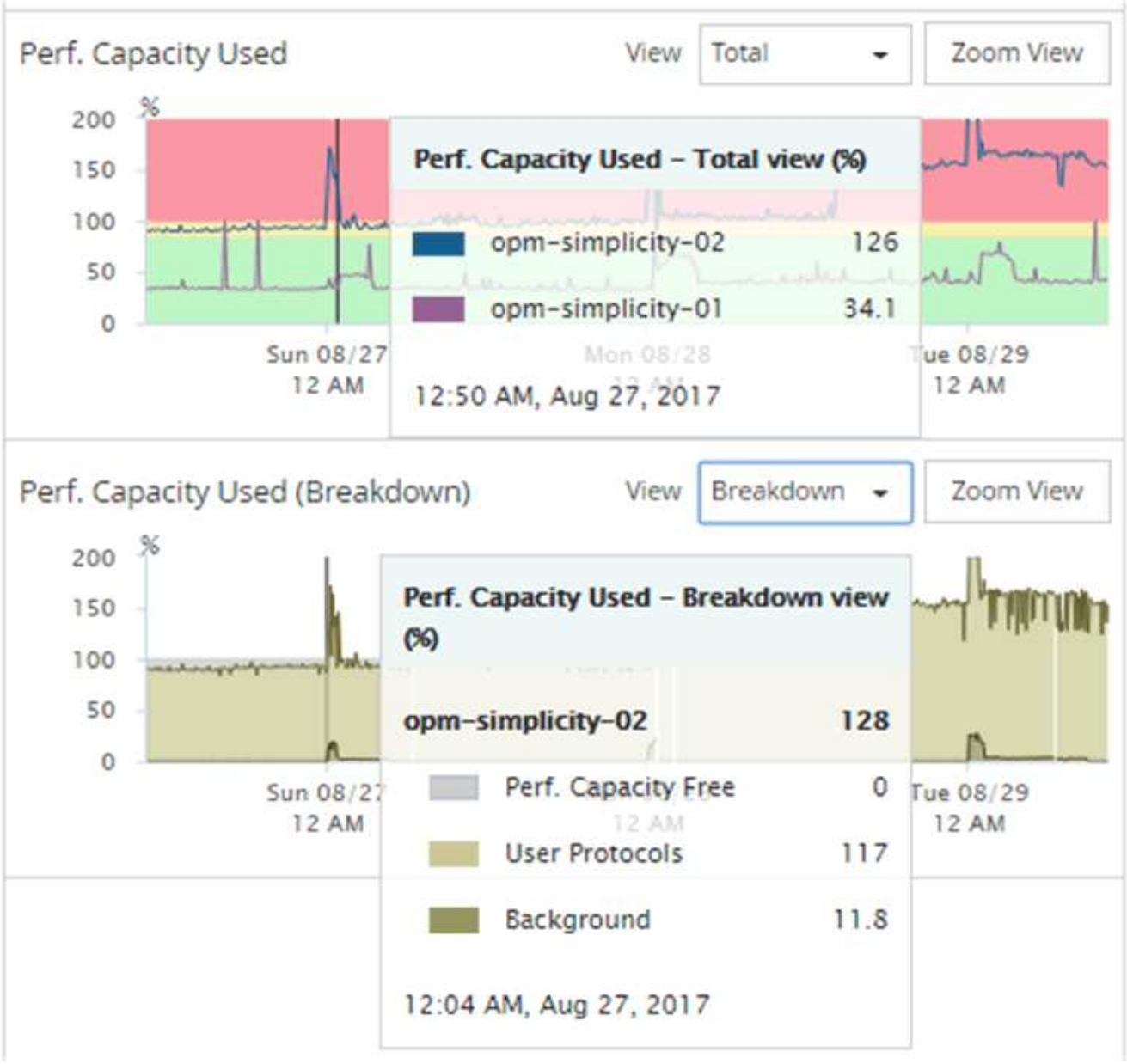
标准计数器图表显示选定节点或聚合的性能容量已用值。细分计数器图表显示根对象的总性能容量值，并按用户协议与后台系统进程的使用情况进行细分。此外，还显示空闲性能容量。

由于与系统和数据管理相关的一些后台活动被标识为用户工作负载并归类为用户协议，因此当这些进程运行时，用户协议百分比可能会显得人为偏高。这些进程通常在集群使用率较低的午夜左右运行。如果您在午夜左右看到用户协议活动激增，请验证集群备份作业或其他后台活动是否配置为在该时间运行。

步骤

1. 从节点或聚合*着陆*页面中选择*资源管理器*选项卡。
2. 在 **Counter Charts** 窗格中，单击 **Choose charts**，然后选择 **Perf.Capacity Used** 图表。
3. 向下滚动，直到您可以查看图表。

   标准图表的颜色显示对象何时处于最佳范围（黄色）、对象何时未充分利用（绿色）以及对象何时过度利用（红色）。细分图表仅显示根对象的详细性能容量详细信息。



4. 如果要以全尺寸格式查看任一图表，请单击*缩放视图*。

   通过这种方式，您可以在单独的窗口中打开多个计数器图表，以比较相同时间范围内的性能容量使用值与 IOPS 或 MBps 值。

在 **Active IQ Unified Manager** 中配置已用性能容量阈值

您可以创建用户定义的性能阈值策略，以便在节点或聚合的性能容量使用值超过定义的性能容量使用阈值设置时触发事件。

此外，可以使用 “使用的性能容量接管” 阈值策略来配置节点。此阈值策略汇总 HA 对中两个节点的使用的性能容量统计信息，以确定如果另一个节点发生故障，其中一个节点是否会缺乏足够的容量。由于故障转移期间的工作负载是两个伙伴节点的工作负载的组合，因此可以将相同的使用的性能容量接管策略应用于两个节点。

这种已用性能容量的等效性在节点之间通常是成立的。但是，如果通过其故障转移配对节点发往其中一个节点的跨节点流量明显更多，则在一个配对节点与另一个配对节点上运行所有工作负载

时所使用的总性能容量可能会略有不同，具体取决于发生故障的节点。

性能容量已用条件还可以用作辅助性能阈值设置，以便在定义 LUN 和卷的阈值时创建组合阈值策略。性能容量已用条件应用于卷或 LUN 所在的聚合或节点。例如，您可以使用以下条件创建组合阈值策略：

存储对象	性能计数器	警告阈值	严重阈值	持续时间
卷	延迟	15 毫秒/操作	25 毫秒/操作	20 分钟
聚合	已使用性能容量	80%	95%	

组合阈值策略仅在整个持续时间内违反两个条件时才会生成事件。

使用 **Active IQ Unified Manager** 中的已用性能容量计数器

通常，组织希望在已用性能容量百分比低于 100 的情况下运行，以便在有效利用资源的同时，保留一些额外的性能容量来支持高峰期的需求。您可以使用阈值策略自定义何时针对高已用性能容量值发送警报。

您可以根据自己的性能要求制定具体目标。例如，金融服务公司可能会保留更多的性能容量，以保证交易的及时执行。这些公司可能希望在 70-80% 的范围内设置已用性能容量阈值。利润率较低的制造公司如果愿意承担性能风险以更好地管理 IT 成本，可能会选择保留较少的性能容量。这些公司可能会在 85-95% 的范围内设置已用性能容量阈值。

当性能容量使用值超过用户定义的阈值策略中设置的百分比时，Unified Manager 会发送警报电子邮件并将事件添加到事件清单页面。这使您能够在潜在问题影响性能之前对其进行管理。这些事件也可用作指标，指示您需要在节点和聚合中进行工作负载移动和更改。

了解并使用节点故障转移规划页面

使用 **Active IQ Unified Manager** 中的节点故障转移规划页面

如果节点的高可用性（HA）配对节点出现故障，“性能/节点故障转移规划”页面将估计对节点的性能影响。Unified Manager 基于 HA 对中节点的历史性能进行估计。

评估故障转移对性能的影响有助于您在以下情况下进行规划：

- 如果故障转移始终将接管节点的估计性能降低到不可接受的水平，则可以考虑采取纠正措施，以减少故障转移对性能的影响。
- 在启动手动故障转移以执行硬件维护任务之前，您可以估计故障转移如何影响接管节点的性能，以确定执行任务的最佳时间。

从 **Active IQ Unified Manager** 的"性能/节点故障转移规划"页面确定纠正措施

根据“性能/节点故障转移计划”页面中显示的信息，您可以采取措施确保故障转移不会导致 HA 对的性能下降到可接受的水平以下。

例如，要降低故障转移的预估性能影响，可以将某些卷或 LUN 从 HA 对中的节点移动到集群中的其他节点。这样做可以确保主节点在故障转移后继续提供可接受的性能。

查看 Active IQ Unified Manager 中 Performance/Node Failover Planning 页面的组件

“性能/节点故障转移计划”页面的组件显示在网格和“比较”窗格中。这些部分使您能够评估节点故障转移对接管节点性能的影响。

性能统计网格

性能/节点故障转移规划页面显示一个包含延迟、IOPS、利用率和已用性能容量统计信息的网格。

> 此页面和“性能/节点性能资源管理器”页面中显示的延迟和 IOPS 值可能不匹配，因为使用不同的性能计数器来计算值以预测节点故障转移。

在网格中，每个节点被分配以下角色之一：

- 主云

  当 HA 配对方发生故障时接管该配对方的节点。根对象始终是主节点。

- 合作伙伴

  在故障转移场景中发生故障的节点。

- 估计接管

  与主节点相同。为此节点显示的性能统计信息显示了接管节点在接管故障配对节点后的性能。

> 虽然接管节点的工作负载相当于故障转移后两个节点的合并工作负载，但预计接管节点的统计数据不是主节点和配对节点统计数据的总和。例如，如果主节点的延迟为 2 ms/op，配对节点的延迟为 3 ms/op，则预计接管节点的延迟可能为 4 ms/op。此值是 Unified Manager 执行的计算。

如果您希望 Partner 节点成为根对象，可以单击该 Partner 节点的名称。显示性能/节点性能资源管理器页面后，您可以单击 故障转移计划 选项卡，查看此节点故障场景中的性能变化情况。例如，如果 Node1 是 Primary 节点，Node2 是 Partner 节点，则可以单击 Node2 将其设置为 Primary 节点。通过这种方式，您可以看到估计的性能如何根据发生故障的节点而变化。

比较窗格

以下列表描述了默认情况下“比较”窗格中显示的组件：

- 事件图表

  它们以与“性能/节点性能资源管理器”页面中相同的格式显示。它们仅与主节点相关。

- 计数器图表

  它们显示网格中显示的性能计数器的历史统计信息。在每个图表中，估计接管节点的图表显示了在任何给定时间发生故障转移时的估计性能。

  例如，假设利用率图表显示预估接管节点在 2 月 8 日上午 11 点的利用率为 73%。如果当时发生了故障转移，则接管节点的利用率将为 73%。

历史统计数据可帮助您找到启动故障转移的最佳时间，最大限度地减少接管节点过载的可能性。您只能在接管节点的预测性能可接受时安排故障转移。

默认情况下，根对象和配对节点的统计信息都显示在“比较”窗格中。与性能/节点性能资源管理器页面不同，此页面不会显示 添加 按钮，供您添加用于统计比较的对象。

您可以像在“性能/节点性能资源管理器”页面中那样自定义“比较”窗格。以下列表显示了自定义图表的示例：

- 单击节点名称可在计数器图表中显示或隐藏该节点的统计信息。
- 单击*缩放视图*以在新窗口中显示特定计数器的详细图表。

在 **Active IQ Unified Manager** 中为节点故障转移规划创建阈值策略

您可以创建节点阈值策略，以便在潜在的故障转移将接管节点的性能降至不可接受的水平时，在“性能/节点故障转移计划”页面中通知您。

名为 “Node HA pair over-utilized” 的系统定义性能阈值策略会在连续六个收集周期（30 分钟）内违反阈值时生成警告事件。如果 HA 对中节点使用的总性能容量超过 200%，则认为该阈值已被违反。

来自系统定义阈值策略的事件提醒您，故障转移将导致接管节点的延迟增加到不可接受的水平。当您看到此策略为特定节点生成的事件时，可以导航到该节点的性能/节点故障转移规划页面，以查看由于故障转移而导致的预测延迟值。

除了使用此系统定义的阈值策略外，您还可以使用 “Performance Capacity Used - Takeover” 计数器创建阈值策略，然后将该策略应用于选定节点。指定低于 200% 的阈值可让您在违反系统定义策略的阈值之前接收事件。如果希望在生成系统定义的策略事件之前收到通知，您还可以将超过阈值的最短时间段指定为小于 30 分钟。

例如，您可以定义一个阈值策略，以便在 HA 对中节点使用的总性能容量超过 175% 且持续 10 分钟以上时生成警告事件。您可以将此策略应用于形成 HA 对的 Node1 和 Node2。收到 Node1 或 Node2 的警告事件通知后，您可以查看该节点的性能/节点故障转移计划页面，以评估对接管节点的估计性能影响。您可以采取纠正措施，以避免在发生故障转移时使接管节点过载。如果在节点使用的总性能容量低于 200% 时采取行动，则即使在此期间发生故障转移，接管节点的延迟也不会达到不可接受的水平。

在 **Active IQ Unified Manager** 中使用已用性能容量明细图表进行故障转移规划

详细的已用性能容量 - 细分图表显示了主节点和配对节点所使用的性能容量。它还显示了预估接管节点上的可用性能容量。此信息可帮助您确定如果配对节点出现故障，是否可能会出现性能问题。

除了显示节点使用的总性能容量外，细分图还将每个节点的值分解为用户协议和后台进程。

- 用户协议是用户应用程序与集群之间的 I/O 操作。
- 后台进程是涉及存储效率、数据复制和系统运行状况的内部系统进程。

这种额外的详细信息级别使您能够确定性能问题是由用户应用程序活动还是后台系统进程引起的，例如重复数据删除、RAID 重建、磁盘清理和 SnapMirror 副本。

步骤

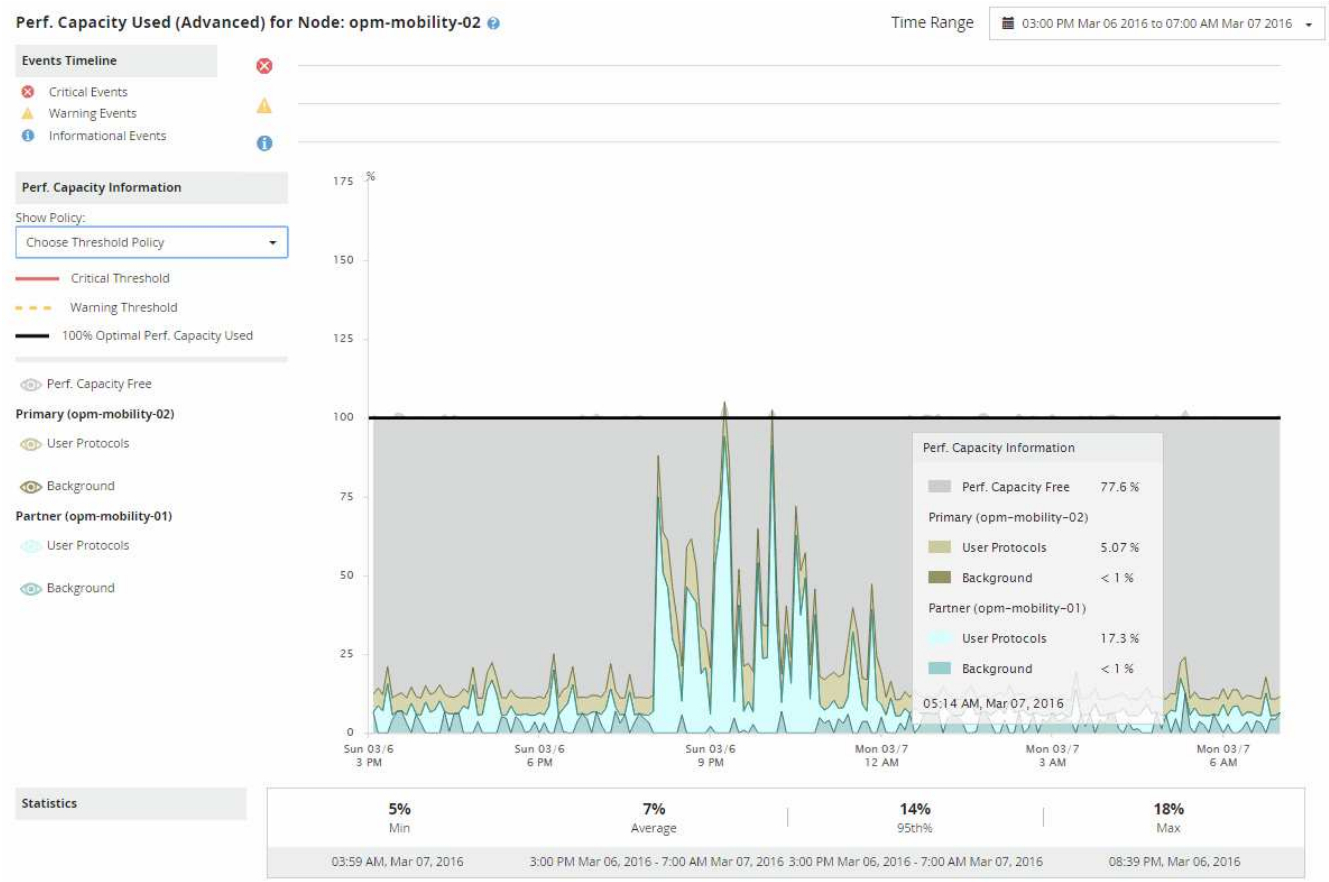
1. 转到将用作 Estimated Takeover 节点的 **Performance/Node Failover Planning** 页面。

2. 从*时间范围*选择器中，选择在计数器网格和计数器图表中显示历史统计信息的时间段。

   此时将显示包含主节点、伙伴节点和预计接管节点统计信息的计数器图表。

3. 从*选择图表*列表中，选择*性能已用容量*。
4. 在*已用性能容量*图表中，选择*明细*，然后单击*缩放视图*。

   此时将显示 Perf.Capacity Used 的详细图表。



5. 将光标移到详细图表上，以在弹出窗口中查看已用性能容量信息。

   Perf.Capacity Free 百分比是估计接管节点上可用的性能容量。它指示故障转移后接管节点上剩余的性能容量。如果为 0%，故障转移将导致接管节点上的延迟增加到不可接受的水平。

6. 考虑采取纠正措施，以避免性能容量空闲百分比过低。

   如果您计划为节点维护启动故障转移，请选择在性能容量空闲百分比不为 0 时使配对节点发生故障的时间。

收集数据并监控工作负载性能

在 **Active IQ Unified Manager** 中收集数据并监控工作负载性能

Unified Manager 每 5 分钟收集和分析一次工作负载活动，以确定性能事件，每 15 分钟检测一次配置更改。它最多保留 30 天的 5 分钟历史性能和事件数据，并使用这些数据来预测所有受监控工作负载的预期延迟范围。

Unified Manager 必须收集至少 3 天的工作负载活动，然后才能开始分析并在“工作负载分析”页面和“事件详细信息”页面上显示 I/O 响应时间的延迟预测。在收集此活动时，延迟预测不会显示工作负载活动发生的所有更改。在收集 3 天的活动后，Unified Manager 会在每 24 小时的凌晨 12:00 调整延迟预测，以反映工作负载活动的变化，并建立更准确的动态性能阈值。

在 Unified Manager 监控工作负载的前 4 天内，如果自上次数据收集以来已超过 24 小时，则延迟图表将不会显示该工作负载的延迟预测。在最后一次收集之前检测到的事件仍然可用。

夏令时 （DST） 会更改系统时间，从而改变受监控工作负载的性能统计信息的延迟预测。Unified Manager 会立即开始更正延迟预测，此过程大约需要 15 天才能完成。在此期间，您可以继续使用 Unified Manager，但由于 Unified Manager 使用延迟预测来检测动态事件，某些事件可能不准确。在时间更改之前检测到的事件不受影响。

使用 **Active IQ Unified Manager** 监控工作负载类型

您可以使用 Unified Manager 监控两种类型工作负载的性能：用户定义和系统定义。

- 用户定义的工作负载

  从应用程序到集群的 I/O 吞吐量。这些是涉及读取和写入请求的进程。卷、LUN、NFS 共享、SMB/CIFS 共享和工作负载是用户定义的工作负载。

  Unified Manager 仅监控集群上的工作负载活动。它不监控应用程序、客户端或应用程序与集群之间的路径。

  如果工作负载符合以下一个或多个条件，则 Unified Manager 无法对其进行监控：

  - 它是只读模式下的数据保护（DP）副本。（会监控 DP 卷是否有用户生成的流量。）
  - 此卷为脱机数据克隆。
  - 此卷为 MetroCluster 配置中的镜像卷。

- 系统定义的工作负载

  与存储效率、数据复制和系统运行状况相关的内部流程，包括：

  - 存储效率，例如重复数据删除
  - 磁盘运行状况，包括 RAID 重建、磁盘清理等
  - 数据复制，例如 SnapMirror 副本
  - 管理活动
  - 文件系统运行状况，包括各种 WAFL 活动
  - 文件系统扫描程序，例如 WAFL 扫描
  - 复制卸载，例如从 VMware 主机卸载存储效率操作
  - 系统运行状况，如卷移动、数据压缩等
  - 不受监控的卷

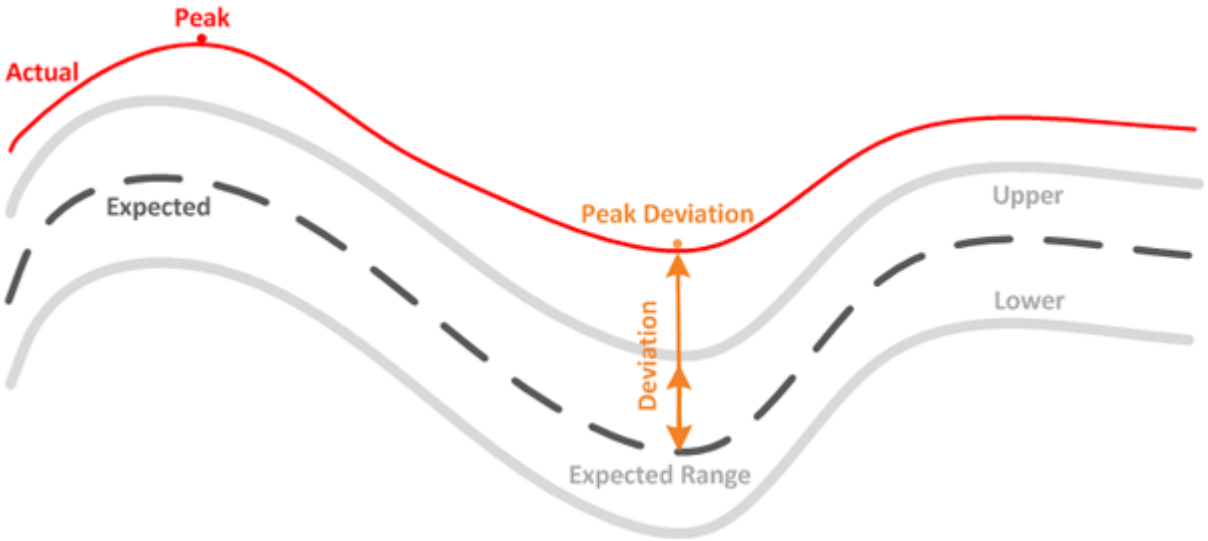
只有当这些工作负载使用的集群组件发生争用时，系统定义的工作负载的性能数据才会显示在 GUI 中。例如，

您无法搜索系统定义的工作负载的名称以在 GUI 中查看其性能数据。

了解 **Active IQ Unified Manager** 中的工作负载性能测量值

Unified Manager 根据历史和预期统计值来衡量集群上工作负载的性能，这些值构成了工作负载的延迟预测值。它将实际工作负载统计值与延迟预测进行比较，以确定工作负载性能何时过高或过低。未按预期执行的工作负载会触发动态性能事件以通知您。

在下图中，红色的实际值表示时间范围内的实际性能统计数据。实际值已超过性能阈值，即延迟预测的上限。峰值是时间范围内的最高实际值。偏差衡量预期值（预测）和实际值之间的变化，而峰值偏差表示预期值和实际值之间的最大变化。



下表列出了工作负载性能测量值。

测量	问题描述
活动	策略组中工作负载使用的 QoS 限制的百分比。 如果 Unified Manager 检测到对策略组的更改，例如添加或删除卷或更改 QoS 限制，则实际值和预期值可能会超过设置限制的 100%。如果某个值超过设定限制的 100%，则显示为 >100%。如果值小于设定限值的 1%，则显示为 <1%。
实际	给定工作负载在特定时间的测量性能值。
偏差	预期值和实际值之间的变化。它是实际值减去预期值与预期范围上限值减去预期值的比率。 负偏差值表示工作负载性能低于预期，而正偏差值表示工作负载性能高于预期。

测量	问题描述
预期	预期值基于对给定工作负载的历史性能数据的分析。Unified Manager 分析这些统计值以确定值的预期范围（延迟预测）。
延迟预测（预期范围）	延迟预测是对特定时间内预期上限和下限性能值的预测。对于工作负载延迟，上限值构成性能阈值。当实际值超过性能阈值时，Unified Manager 会触发动态性能事件。
峰值	在一段时间内测量的最大值。
峰值偏差	在一段时间内测量的最大偏差值。
队列深度	在互连组件处等待的挂起 I/O 请求数。
利用率	对于网络处理、数据处理和聚合组件，在一段时间内完成工作负载操作的忙碌时间百分比。例如，网络处理或数据处理组件处理 I/O 请求或聚合完成读取或写入请求的时间百分比。
写入吞吐量	从本地集群上的工作负载到 MetroCluster 配置中的配对集群的写入吞吐量，以兆字节/秒（MB/s）为单位。

了解 **Active IQ Unified Manager** 如何计算预期性能范围

延迟预测是对特定时间内预期上限和下限性能值的预测。对于工作负载延迟，上限值构成性能阈值。当实际值超过性能阈值时，Unified Manager 会触发动态性能事件。

例如，在上午 9:00 至下午 5:00 的正常工作时间内，大多数员工可能会在上午 9:00 至上午 10:30 之间查看电子邮件。对电子邮件服务器的需求增加意味着在此期间后端存储的工作负载活动增加。员工可能会注意到电子邮件客户端的响应时间很慢。

在中午 12:00 至下午 1:00 之间的午餐时间以及下午 5:00 之后的工作日结束时，大多数员工可能会离开电脑。对电子邮件服务器的需求通常会下降，同时也会降低对后端存储的需求。或者，可能会有计划内的工作负载操作，例如存储备份或病毒扫描，这些操作在下午 5:00 之后开始，并增加后端存储上的活动。

在几天内，工作负载活动的增加和减少决定了活动的预期范围（延迟预测），以及工作负载的上限和下限。当对象的实际工作负载活动在上限或下限之外，并且在一段时间内保持在边界之外时，这可能表明对象被过度使用或未充分使用。

延迟预测是如何形成的

Unified Manager 必须收集至少 3 天的工作负载活动，然后才能开始分析，并且才能在 GUI 中显示 I/O 响应时间的延迟预测。最低要求的数据收集不考虑工作负载活动发生的所有更改。在收集前 3 天的活动后，Unified Manager 会在每 24 小时的凌晨 12:00 调整延迟预测，以反映工作负载活动的变化，并建立更准确的动态性能阈值。

夏令时 （DST） 会更改系统时间，从而改变受监控工作负载的性能统计信息的延迟预测。Unified Manager 会立即开始更正延迟预测，此过程大约需要 15 天才能完成。在此期间，您可以继续使用 Unified Manager，但由于 Unified Manager 使用延迟预测来检测动态事件，某些事件可能不准确。在时间更改之前检测到的事件不受影响。

使用 **Active IQ Unified Manager** 中的延迟预测进行性能分析

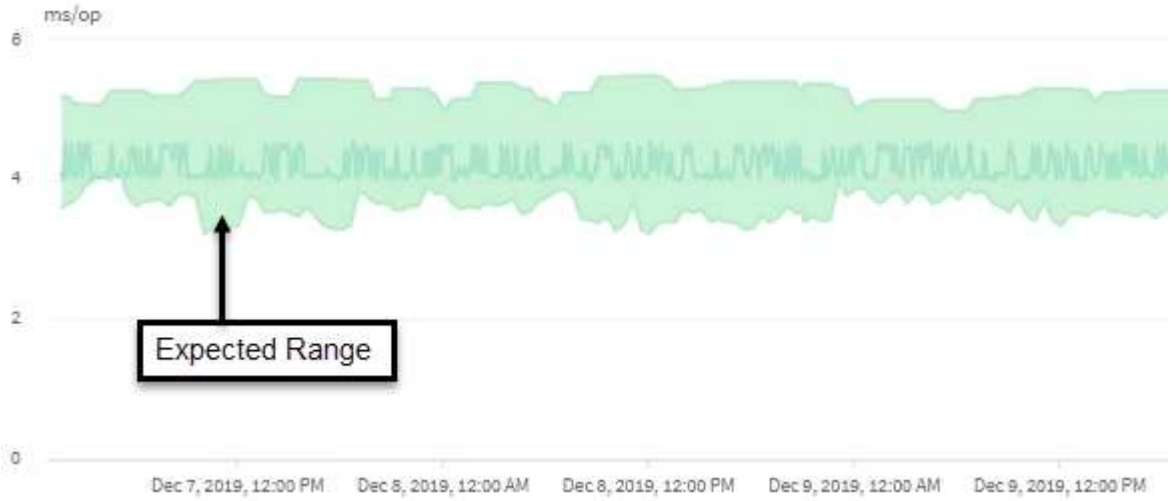
Unified Manager 使用延迟预测来表示受监控工作负载的典型 I/O 延迟（响应时间）活动。当工作负载的实际延迟高于延迟预测的上限时，它会向您发出警报，从而触发动态性能事件，以便您可以分析性能问题并采取纠正措施来解决该问题。

延迟预测设置工作负载的性能基线。随着时间的推移，Unified Manager 会从过去的性能测量中学习，以预测工作负载的预期性能和活动水平。预期范围的上边界建立动态性能阈值。Unified Manager 使用基线来确定实际延迟何时高于或低于阈值，或超出其预期范围的界限。实际值和预期值之间的比较为工作负载创建了性能配置文件。

当工作负载的实际延迟超过动态性能阈值时，由于集群组件上的争用，延迟会很高，并且工作负载的运行速度会比预期的慢。共享相同集群组件的其他工作负载的性能也可能比预期的慢。

Unified Manager 会分析阈值跨越事件，并确定该活动是否为性能事件。如果高工作负载活动在很长一段时间内保持一致，例如几个小时，Unified Manager 会认为该活动正常，并动态调整延迟预测以形成新的动态性能阈值。

某些工作负载可能一直处于低活动状态，其延迟预测随时间推移的变化率不高。为了在分析性能事件期间最大限度地减少事件数量，Unified Manager 仅针对操作和延迟远高于预期的低活动卷触发事件。



在此示例中，卷的延迟预测（以灰色表示）最低为 3.5 毫秒/次操作（ms/op），最高为 5.5 ms/op。如果由于网络流量的间歇性激增或集群组件上的争用，实际延迟（以蓝色表示）突然增加到 10 ms/op，则它将高于延迟预测，并超过动态性能阈值。

当网络流量减少或集群组件不再处于竞争状态时，延迟将返回到延迟预测范围内。如果延迟长时间保持在 10 ms/op 或以上，则可能需要采取纠正措施来解决此事件。

使用工作负载延迟识别 **Active IQ Unified Manager** 中的性能问题

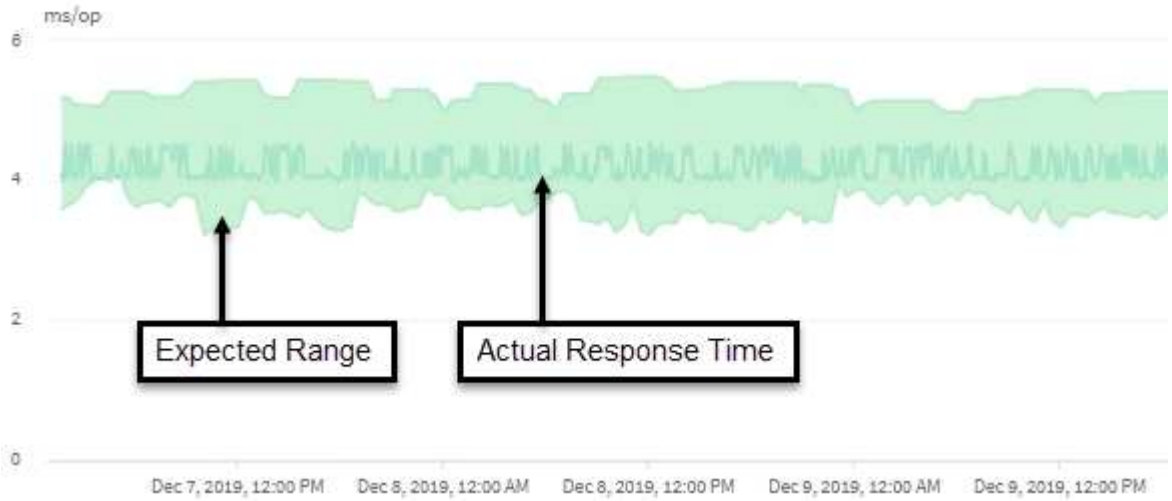
工作负载延迟（响应时间）是群集上的卷响应来自客户端应用程序的 I/O 请求所花费的时间。Unified Manager 使用延迟来检测性能事件并提醒您。

高延迟意味着从应用程序到集群上的卷的请求花费的时间比平常更长。高延迟的原因可能在集群本身，这是由于一个或多个集群组件上存在争用。高延迟也可能是由集群外部的问题引起的，例如网络瓶颈、托管应用程序的客户端问题或应用程序本身的问题。

Unified Manager 仅监控集群上的工作负载活动。它不监控应用程序、客户端或应用程序与集群之间的路径。

集群上的操作（例如进行备份或运行重复数据删除）增加了对其他工作负载共享的集群组件的需求，也可能导致高延迟。如果实际延迟超过预期范围的动态性能阈值（延迟预测），Unified Manager 将分析事件以确定它是否是您可能需要解决的性能事件。延迟以每次操作的毫秒数（ms/op）为单位进行测量。

在“工作负载分析”页面的“总延迟”图表上，您可以查看延迟统计数据的分析，以查看单个进程（如读取和写入请求）的活动与整体延迟统计数据的比较情况。此比较可帮助您确定哪些操作的活动最高，或者特定操作是否具有影响卷延迟的异常活动。在分析性能事件时，您可以使用延迟统计数据来确定事件是否由集群上的问题引起。您还可以识别事件中涉及的特定工作负载活动或集群组件。



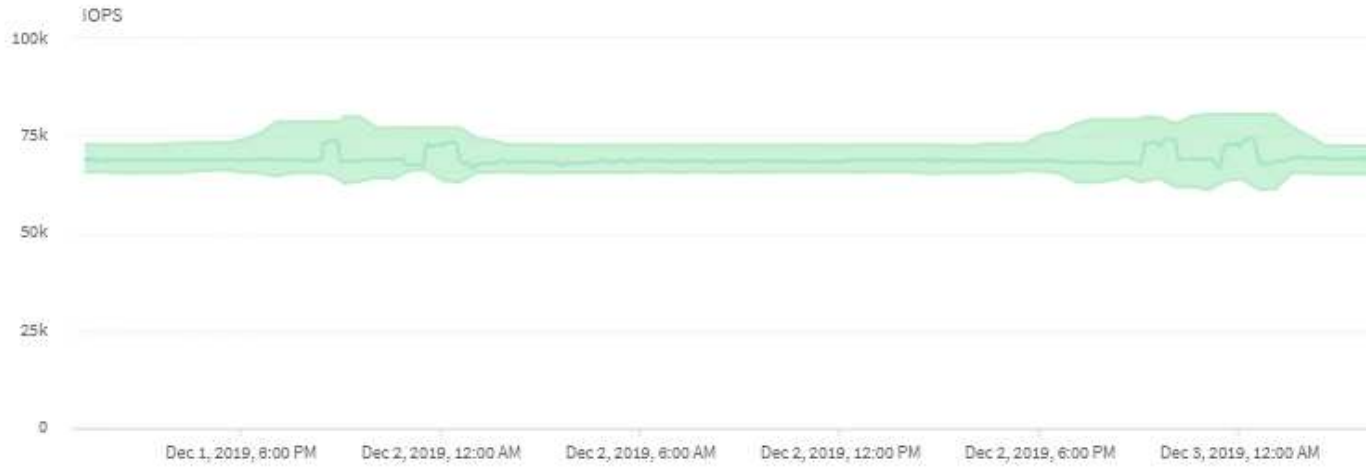
此示例显示了延迟图表。实际响应时间（延迟）活动为蓝线，延迟预测（预期范围）为绿色。

如果 Unified Manager 无法收集数据，蓝线中可能存在间隙。出现这种情况的原因可能是无法访问集群或卷，在此期间关闭了 Unified Manager，或者收集时间超过了 5 分钟的收集周期。

评估集群操作如何影响 **Active IQ Unified Manager** 中的工作负载延迟

操作（IOPS）表示集群上所有用户定义和系统定义工作负载的活动。IOPS 统计数据可帮助您确定集群进程（如进行备份或运行重复数据删除）是否影响工作负载延迟（响应时间），或者是否可能导致或促成了性能事件。

在分析性能事件时，您可以使用 IOPS 统计信息来确定性能事件是否由集群上的问题引起。您可以确定可能是性能事件主要促成因素的特定工作负载活动。IOPS 以每秒操作数（ops/sec）衡量。



此示例显示了 IOPS 图表。实际操作统计数据为蓝线，操作统计数据的 IOPS 预测为绿线。

在某些情况下，如果集群超载，Unified Manager 可能会显示消息 `Data collection is taking too long on Cluster cluster_name`。这意味着没有收集足够的统计数据供 Unified Manager 进行分析。您需要减少集群正在使用的资源，以便可以收集统计信息。

使用 **Active IQ Unified Manager** 监控 **MetroCluster** 性能

Unified Manager 使您能够监控 MetroCluster 配置中集群之间的写入吞吐量，以识别具有高写入吞吐量的工作负载。

如果这些高性能工作负载导致本地集群上的其他卷具有较高的 I/O 响应时间，则 Unified Manager 会触发性能事件以通知您。

Unified Manager 将 MetroCluster 配置中的集群视为单独的集群。它不区分互为配对的集群，也不关联每个集群的写入吞吐量。

当 MetroCluster 配置中的本地群集将其数据镜像到其伙伴群集时，数据将写入 NVRAM，然后通过交换机间链路（ISL）传输到远程聚合。Unified Manager 分析 NVRAM 以识别高写入吞吐量过度使用 NVRAM 的工作负载，从而使 NVRAM 处于争用状态。

响应时间偏差超过性能阈值的工作负载称为 *victims*，而对 NVRAM 的写入吞吐量偏差高于平时并导致争用的工作负载称为 *bullies*。由于只有写入请求才会镜像到配对集群，因此 Unified Manager 不会分析读取吞吐量。

您可以通过从以下屏幕分析相应 LUN 和卷的工作负载来查看 MetroCluster 配置中任何集群的吞吐量。您可以按集群筛选结果。在左侧导航窗格中：

- *存储 > 集群 > 性能：所有集群*视图。请参阅
- *存储 > 卷 > 性能：所有卷*视图。
- 存储 **> LUN >** 性能：所有**LUN** 视图。
- 工作负载分析 **>** 所有工作负载

相关信息

"性能事件分析和通知"

"MetroCluster 配置的性能事件分析"

"性能事件中涉及的工作负载的角色"

"识别性能事件中涉及的受害工作负载"

"识别性能事件中涉及的恶霸工作负载"

"识别性能事件中涉及的 shark 工作负载"

了解性能事件和警报

了解 **Active IQ Unified Manager** 中的性能事件和警报

性能事件是与集群上的工作负载性能相关的事件。它们可帮助您识别响应时间较慢的工作负载。结合同时发生的运行状况事件，您可以确定可能导致或促成响应时间缓慢的问题。

当 Unified Manager 检测到同一集群组件出现多次相同事件条件时，它会将所有事件视为单个事件，而不是单独的事件。

您可以配置警报，以便在发生某些严重性类型的性能事件时自动发送电子邮件通知。

确定 **Active IQ Unified Manager** 中性能事件的来源

性能事件是与集群上的工作负载性能相关的问题。它们可帮助您识别响应时间较慢的存储对象，也称为高延迟。结合同时发生的其他运行状况事件，您可以确定可能导致或促成响应时间缓慢的问题。

Unified Manager 从下列来源接收性能事件：

- 用户定义的性能阈值策略事件

  基于您设置的自定义阈值的性能问题。您可以为存储对象（例如聚合和卷）配置性能阈值策略，以便在超过性能计数器的阈值时生成事件。

  必须定义性能阈值策略并将其分配给存储对象以接收这些事件。

- 系统定义的性能阈值策略事件

  基于系统定义的阈值的性能问题。这些阈值策略包含在 Unified Manager 的安装中，以涵盖常见的性能问题。

  默认情况下会启用这些阈值策略，您可能会在添加集群后不久看到事件。

- 动态性能阈值事件

  由于 IT 基础架构中的故障或错误，或由于工作负载过度使用集群资源而导致的性能问题。这些事件的原因可能是一个简单的问题，可以在一段时间内自行纠正，也可以通过修复或配置更改来解决。动态阈值事件表示，由于其他工作负载对共享集群组件的使用率较高，ONTAP 系统上的工作负载速度较慢。

默认情况下会启用这些阈值，从新集群收集数据三天后，您可能会看到事件。

在 Active IQ Unified Manager 中按严重性对性能事件进行优先级排序

每个性能事件都与严重程度类型相关联，以帮助您对需要立即采取纠正措施的事件进行优先级排序。

- 严重

  发生了一个性能事件，如果不立即采取纠正措施，可能会导致服务中断。

  严重事件仅从用户定义的阈值发送。

- 警告

  集群对象的性能计数器超出正常范围，应进行监控以确保其未达到严重级别。此严重级别的事件不会导致服务中断，可能不需要立即采取纠正措施。

  警告事件从用户定义、系统定义或动态阈值发送。

- 信息

  当发现新对象或执行用户操作时，会发生此事件。例如，当删除任何存储对象或发生任何配置更改时，将生成严重性类型为“信息”的事件。

  当检测到配置更改时，信息事件将直接从 ONTAP 发送。

有关详细信息，请参见以下链接：

- "收到事件时会发生什么情况"
- "警报电子邮件中包含哪些信息"
- "添加警报"
- "为性能事件添加警报"

监控 Active IQ Unified Manager 检测到的配置更改

Unified Manager 监控您的集群的配置更改，以帮助您确定更改是否可能导致或促成性能事件。性能资源管理器页面显示更改事件图标（），以指示检测到更改的日期和时间。

您可以在“性能资源管理器”页面和“工作负载分析”页面中查看性能图表，以查看更改事件是否影响所选集群对象的性能。如果在性能事件发生的同时或前后检测到更改，则该更改可能是导致问题的原因，从而触发了事件警报。

Unified Manager 可以检测到以下变更事件，这些事件被归类为信息事件：

- 卷在聚合之间移动。

  Unified Manager 可以检测移动是正在进行、已完成还是已失败。如果 Unified Manager 在卷移动期间停止运行，则在恢复运行时，它会检测到卷移动并为其显示一个更改事件。

- 包含一个或多个受监控工作负载的 QoS 策略组的吞吐量（MB/s 或 IOPS）限制发生更改。

  更改策略组限制可能会导致延迟（响应时间）出现间歇性峰值，这也可能触发策略组的事件。延迟会逐渐恢复正常，由峰值引起的任何事件都会过时。

- HA 对中的节点接管或交还其伙伴节点的存储。

  Unified Manager 可以检测接管、部分接管或交还操作何时完成。如果接管是由崩溃的节点引起的，则 Unified Manager 不会检测到该事件。

- 已成功完成 ONTAP 升级或还原操作。

  将显示先前版本和新版本。

了解 **Active IQ Unified Manager** 中系统定义的性能阈值策略

Unified Manager 提供一些标准阈值策略，可监控集群性能并自动生成事件。默认情况下，这些策略处于启用状态，当超出受监控的性能阈值时，它们会生成警告或信息事件。

Cloud Volumes ONTAP、ONTAP Edge 或 ONTAP Select 系统上未启用系统定义的性能阈值策略。

如果从任何系统定义的性能阈值策略接收到不必要的事件，则可以从“事件设置”页面禁用单个策略的事件。

集群阈值策略

默认情况下，系统定义的集群性能阈值策略分配给由 Unified Manager 监控的每个集群：

- 集群负载不平衡

  识别一个节点在比集群中的其他节点高得多的负载下运行的情况，从而可能影响工作负载延迟。

  它通过比较集群中所有节点的性能容量使用值来实现此目的，以查看是否有任何节点超过 30% 阈值的时间超过 24 小时。这是一个警告事件。

- 集群容量不平衡

  标识一个聚合的使用容量远高于集群中其他聚合的情况，因此可能会影响操作所需的空间。

  它通过比较集群中所有聚合的已用容量值来实现此目的，以查看任何聚合之间是否存在 70% 的差异。这是一个警告事件。

节点阈值策略

默认情况下，系统定义的节点性能阈值策略会分配给由 Unified Manager 监控的集群中的每个节点：

- 已违反已用性能容量阈值

  识别单个节点运行超出其运行效率界限的情况，从而可能影响工作负载延迟。

  它通过查找使用超过 100% 的性能容量且持续超过 12 小时的节点来实现此目的。这是一个警告事件。

- 节点 **HA** 对已过度利用

  确定 HA 对中的节点运行效率高于 HA 对运行效率范围的情况。

  它通过查看 HA 对中两个节点的性能容量使用值来实现此目的。如果两个节点使用的总性能容量超过 200% 且持续 12 小时以上，则控制器故障转移将影响工作负载延迟。这是一个信息事件。

- 节点磁盘碎片

  识别聚合中的一个或多个磁盘碎片化，减慢关键系统服务并可能影响节点上工作负载延迟的情况。

  它通过查看节点上所有聚合的某些读取和写入操作比率来实现。在 SyncMirror 重新同步期间或在磁盘清理操作期间发现错误时，也可能会触发此策略。这是一个警告事件。

  "\`节点磁盘碎片\`" 策略分析仅限 HDD 的聚合；不分析 Flash Pool、SSD 和 FabricPool 聚合。

聚合阈值策略

系统定义的聚合性能阈值策略默认分配给由 Unified Manager 监控的集群中的每个聚合：

- 聚合磁盘使用过度

  识别聚合运行超出其运行效率限制的情况，从而可能影响工作负载延迟。它通过查找聚合中的磁盘利用率超过 95% 且持续时间超过 30 分钟的聚合来识别这些情况。然后，此多条件策略将执行以下分析以帮助确定问题的原因：

  - 聚合中的磁盘当前是否正在进行后台维护活动？

    磁盘可能正在进行的一些后台维护活动包括磁盘重建、磁盘清理、SyncMirror 重新同步和重新计算奇偶校验。

  - 磁盘架光纤通道互连中是否存在通信瓶颈？
  - 聚合中的可用空间是否太少？仅当三个从属策略中的一个（或多个）也被视为违规时，才会为此策略发出警告事件。如果只有聚合中的磁盘利用率超过 95%，则不会触发性能事件。

“聚合磁盘过度使用”策略分析仅 HDD 聚合和 Flash Pool（混合）聚合；不分析 SSD 和 FabricPool 聚合。

工作负载延迟阈值策略

系统定义的工作负载延迟阈值策略将分配给具有已配置性能服务级别策略的任何工作负载，该策略具有定义的“expected latency” 值：

- 已违反性能服务级别定义的工作负载卷**/LUN** 延迟阈值

  标识已超出“预期延迟”限制且影响工作负载性能的卷（文件共享）和 LUN。这是一个警告事件。

  它通过查找在过去一小时内有 30% 的时间超过预期延迟值的工作负载来实现此目的。

QoS 阈值策略

系统定义的 QoS 性能阈值策略将分配给配置了 ONTAP QoS 最大吞吐量策略（IOPS、IOPS/TB 或 MB/s）的任何工作负载。当工作负载吞吐量值比配置的 QoS 值低 15% 时，Unified Manager 会触发事件：

- **QoS** 最大 **IOPS** 或 **MB/s** 阈值

  标识已超出其 QoS 最大 IOPS 或 MB/s 吞吐量限制并影响工作负载延迟的卷和 LUN。这是一个警告事件。

  将单个工作负载分配给策略组时，它通过查找在前一小时的每个收集期间超过分配的 QoS 策略组中定义的最大吞吐量阈值的工作负载来实现此目的。

  当多个工作负载共享单个 QoS 策略时，它通过将该策略中所有工作负载的 IOPS 或 MB/s 相加，并将该总数与阈值进行比较来实现这一点。

- **QoS** 峰值 **IOPS/TB** 或带有块大小阈值的 **IOPS/TB**

  标识已超过其自适应 QoS 峰值 IOPS/TB 吞吐量限制（或带块大小限制的 IOPS/TB），且正在影响工作负载延迟的卷。这是一个警告事件。

  为此，它根据每个卷的大小将自适应 QoS 策略中定义的峰值 IOPS/TB 阈值转换为 QoS 最大 IOPS 值，然后查找在前一小时的每个性能收集期间超过 QoS 最大 IOPS 的卷。

  仅当集群安装了 ONTAP 9.3 及更高版本软件时，此策略才应用于卷。

  当自适应 QoS 策略中定义了"`block size`"元素时，系统会根据每个卷的大小将阈值转换为 QoS 最大 MB/s 值。然后，系统会查找在前一小时内每个性能收集周期中超过 QoS 最大 MB/s 的卷。

  仅当集群安装了 ONTAP 9.5 及更高版本软件时，此策略才应用于卷。

分析 **Active IQ Unified Manager** 中的性能事件和通知

性能事件会通知您由集群组件上的争用引起的工作负载上的 I/O 性能问题。Unified Manager 将分析事件，以确定所涉及的所有工作负载、发生争用的组件以及事件是否仍然是您可能需要解决的问题。

Unified Manager 监控集群上卷的 I/O 延迟（响应时间）和 IOPS（操作）。例如，当其他工作负载过度使用集群组件时，该组件会处于争用状态，无法以最佳水平运行来满足工作负载需求。使用相同组件的其他工作负载的性能可能会受到影响，从而导致其延迟增加。如果延迟超过动态性能阈值，Unified Manager 将触发性能事件以通知您。

事件分析

Unified Manager 使用过去 15 天的性能统计信息执行以下分析，以确定事件中涉及的受害工作负载、恶霸工作负载和集群组件：

- 识别延迟超过动态性能阈值的受害者工作负载，动态性能阈值是延迟预测的上限：
  - 对于 HDD 或 Flash Pool 混合聚合（本地层）上的卷，仅当延迟大于 5 毫秒（ms）且 IOPS 大于每秒 10 次操作（ops/sec）时才会触发事件。
  - 对于全 SSD 聚合或 FabricPool 聚合（云层）上的卷，仅当延迟大于 1 ms 且 IOPS 大于 100 ops/sec 时

才会触发事件。

- 标识争用中的集群组件。

  如果集群互连处的受害工作负载延迟大于 1 毫秒，Unified Manager 会将其视为重大问题，并触发集群互连事件。

- 标识过度使用集群组件并导致其处于争用状态的欺凌工作负载。
- 根据集群组件利用率或活动的偏差对所涉及的工作负载进行排名，以确定哪些欺凌者对集群组件的使用率变化最大，哪些受害者受到的影响最大。

事件可能仅发生短暂的时间，并在其使用的组件不再发生争用后自行恢复。连续事件是指在五分钟间隔内对同一集群组件重复发生并保持活动状态的事件。对于连续事件，Unified Manager 在连续两个分析间隔期间检测到同一事件后会触发警报。

当事件解决后，它在 Unified Manager 中仍然可用，作为卷过去性能问题记录的一部分。每个事件都有一个唯一的 ID，用于标识事件类型以及所涉及的卷、集群和集群组件。

单个卷可以同时涉及多个事件。

事件状态

事件可能处于以下状态之一：

- 活动

  指示性能事件当前处于活动状态（新建或已确认）。导致事件的问题尚未自行更正或尚未解决。存储对象的性能计数器仍高于性能阈值。

- 已废弃

  指示该事件不再处于活动状态。导致该事件的问题已自行更正或已解决。存储对象的性能计数器不再高于性能阈值。

事件通知

事件显示在“仪表板”页面和用户界面的许多其他页面上，这些事件的警报将发送到指定的电子邮件地址。您可以在“事件详细信息”页面和“工作负载分析”页面上查看有关事件的详细分析信息并获取解决该事件的建议。

事件交互

在“事件详细信息”页面和“工作负载分析”页面上，您可以通过以下方式与事件进行交互：

- 将鼠标移到事件上会显示一条消息，显示检测到事件的日期和时间。

  如果同一时间段存在多个事件，消息将显示事件数量。

- 单击单个事件将显示一个对话框，其中显示有关该事件的更详细信息，包括所涉及的集群组件。

  竞争中的组件以红色圆圈突出显示。您可以单击 **View full analysis** 以在 Event details 页面上查看完整分析。如果同一时间段内存在多个事件，该对话框将显示最近三个事件的详细信息。您可以单击某个事件，以

在 Event details 页面上查看事件分析。

了解 **Active IQ Unified Manager** 如何确定事件的性能影响

Unified Manager 使用工作负载的活动、利用率、写入吞吐量、集群组件使用率或 I/O 延迟（响应时间）的偏差来确定对工作负载性能的影响程度。这些信息决定了每个工作负载在事件中的角色以及它们在事件详细信息页面上的排名方式。

Unified Manager 将工作负载的最后分析值与值的预期范围（延迟预测）进行比较。上次分析的值与预期值范围之间的差异标识了性能受事件影响最大的工作负载。

例如，假设集群包含两个工作负载：工作负载 A 和工作负载 B。工作负载 A 的延迟预测为每次操作 5-10 毫秒（ms/op），其实际延迟通常约为 7 ms/op。工作负载 B 的延迟预测为 10-20 ms/op，其实际延迟通常约为 15 ms/op。这两个工作负载都在其延迟预测范围内。由于集群上的竞争，两个工作负载的延迟都增加到 40 ms/op，跨越了动态性能阈值（即延迟预测的上限），并触发了事件。工作负载 A 的延迟偏差（从预期值到高于性能阈值的值）约为 33 ms/op，工作负载 B 的偏差约为 25 ms/op。两个工作负载的延迟均飙升至 40 ms/op，但工作负载 A 对性能的影响更大，因为它的延迟偏差更高，达到了 33 ms/op。

在“事件详细信息”页面的“系统诊断”部分，您可以按集群组件的活动、利用率或吞吐量偏差对工作负载进行排序。您还可以按延迟对工作负载进行排序。当您选择排序选项时，Unified Manager 会分析自检测到事件以来活动、利用率、吞吐量或延迟与预期值的偏差，以确定工作负载的排序顺序。对于延迟，红点（🔴）表示受害工作负载超出了性能阈值，以及随后对延迟产生的影响。每个红点表示更高水平的延迟偏差，这有助于您识别延迟受事件影响最大的受害工作负载。

了解 **Active IQ Unified Manager** 中的集群组件和争用情况

当集群组件发生争用时，您可以识别集群性能问题。使用该组件的工作负载性能会下降，其对客户端请求的响应时间（延迟）会增加，这会在 Unified Manager 中触发事件。

处于争用状态的组件无法在最佳水平下运行。其性能会有所下降，并且其他集群组件和工作负载（称为 *victims* ）的性能可能会出现延迟增加的情况。要使组件摆脱争用状态，必须减少其工作负载或提高其处理更多工作的能力，以便性能能够恢复到正常水平。由于 Unified Manager 每隔五分钟收集并分析一次工作负载性能，因此它仅在集群组件被持续过度使用时才会检测到。在五分钟间隔内仅持续很短时间的暂时性过度使用峰值不会被检测到。

例如，存储聚合可能存在争用，因为其上的一个或多个工作负载正在争用以满足其 I/O 请求。聚合上的其他工作负载可能会受到影响，导致其性能下降。为了减少聚合上的活动量，您可以采取不同的步骤，例如将一个或多个工作负载移动到不太繁忙的聚合或节点，以减少当前聚合的整体工作负载需求。对于 QoS 策略组，您可以调整吞吐量限制，或将工作负载移动到其他策略组，以便不再限制工作负载。

Unified Manager 可监控以下集群组件，以便在它们发生争用时向您发出警报：

- 网络

  表示集群上外部网络协议对 I/O 请求的等待时间。等待时间是指集群在对 I/O 请求做出响应前等待 “transfer ready” 事务完成的时间。如果网络组件存在争用，则意味着协议层的等待时间过长会影响一个或多个工作负载的延迟。

- 网络处理

  表示集群中涉及协议层和集群之间 I/O 处理的软件组件。自检测到事件以来，负责网络处理的节点可能已发生更改。如果网络处理组件处于争用状态，则意味着网络处理节点的高利用率正在影响一个或多个工作负载

的延迟。

在双活配置中使用全 SAN 阵列集群时，将显示两个节点的网络处理延迟值，以便您验证节点是否平均分担负载。

- 服务质量（**QoS**）上限

  表示分配给工作负载的存储服务质量（QoS）策略组的吞吐量最大值（峰值）设置。如果策略组组件存在争用，则表示策略组中的所有工作负载都受到设置的吞吐量限制的限制，这会影响其中一个或多个工作负载的延迟。

- **QoS** 限制下限

  表示分配给其他工作负载的 QoS 吞吐量最小（预期）设置导致的工作负载延迟。如果在某些工作负载上设置的 QoS 最小值使用了大部分带宽来保证承诺的吞吐量，则其他工作负载将受到限制并出现更高的延迟。

- 集群互连

  表示与已加入集群的节点物理连接的缆线和适配器。如果集群互连组件处于争用状态，则意味着在集群互连处等待 I/O 请求的时间较长，这会影响一个或多个工作负载的延迟。

- **Data Processing**

  表示集群中涉及集群和包含工作负载的存储聚合之间的 I/O 处理的软件组件。负责 Data Processing 的节点可能会在检测到事件后发生更改。如果 Data Processing 组件存在争用，则意味着 Data Processing 节点的高利用率会影响一个或多个工作负载的延迟。

- 卷激活

  表示跟踪所有活动卷使用情况的过程。在超过 1000 个卷处于活动状态的大型环境中，此过程将跟踪有多少关键卷需要同时通过节点访问资源。当并发活动卷的数量超过建议的最大阈值时，某些非关键卷将出现此处指出的延迟。

- **MetroCluster** 资源

  表示 MetroCluster 资源，包括 NVRAM 和交换机间链路（ISL），用于在 MetroCluster 配置中的集群之间镜像数据。如果 MetroCluster 组件存在争用，则意味着本地集群上工作负载的高写入吞吐量或链路运行状况问题正在影响本地集群上一个或多个工作负载的延迟。如果集群不在 MetroCluster 配置中，则不显示此图标。

- 聚合或 **SSD** 聚合操作

  表示运行工作负载的存储聚合。如果聚合组件存在争用，则意味着聚合的高利用率正在影响一个或多个工作负载的延迟。聚合由全部 HDD，或者 HDD 和 SSD 的混合（Flash Pool 聚合），或者 HDD 和云层的混合（FabricPool 聚合）组成。“SSD Aggregate” 由全部 SSD（全闪存聚合），或者 SSD 和云层的混合（FabricPool 聚合）组成。

- 云延迟

  表示集群和存储用户数据的云层之间的 I/O 处理所涉及的软件组件。如果云延迟组件发生争用，则意味着从云层上托管的卷进行的大量读取会影响一个或多个工作负载的延迟。

- 同步 **SnapMirror**

表示集群中涉及在 SnapMirror 同步关系中将用户数据从主卷复制到辅助卷的软件组件。如果同步 SnapMirror 组件存在争用，则表示来自 SnapMirror 同步操作的活动正在影响一个或多个工作负载的延迟。

在 **Active IQ Unified Manager** 中识别性能事件中的工作负载角色

Unified Manager 使用角色来识别工作负载在性能事件中的参与度。角色包括受害者、欺凌者和鲨鱼。用户定义的工作负载可能同时是受害者、欺凌者和鲨鱼。

角色	问题描述
受影响	由于过度使用集群组件的其他工作负载（称为恶霸）而导致性能下降的用户定义工作负载。仅将用户定义的工作负载标识为受害者。Unified Manager 根据延迟的偏差来识别受害者工作负载，其中事件期间的实际延迟比其延迟预测（预期范围）大大增加。
抢占资源	用户定义或系统定义的工作负载，其过度使用集群组件导致其他工作负载（称为受害者）的性能降低。Unified Manager 根据集群组件的使用偏差来识别欺凌工作负载，其中在事件期间的实际使用量比其预期的使用范围大大增加。
强占资源的工作负载	与事件中涉及的所有工作负载相比，集群组件的使用率最高的用户定义工作负载。Unified Manager 根据事件期间集群组件的使用情况来识别 shark 工作负载。

集群上的工作负载可以共享许多集群组件，例如用于网络和数据处理的聚合和 CPU。当工作负载（如卷）增加其对集群组件的使用，以至于组件无法有效地满足工作负载需求时，该组件就处于争用状态。过度使用集群组件的工作负载是欺凌者。共享这些组件且其性能受到欺凌者影响的其他工作负载是受害者。来自系统定义工作负载（例如重复数据删除或 Snapshot 副本）的活动也可能升级为 “bullying”。

当 Unified Manager 检测到事件时，它会识别所涉及的所有工作负载和集群组件，包括导致事件的恶霸工作负载、发生争用的集群组件以及由于恶霸工作负载的活动增加而导致性能下降的受害者工作负载。

如果 Unified Manager 无法识别恶霸工作负载，它只会对受害者工作负载和所涉及的集群组件发出警报。

Unified Manager 可以识别作为欺凌工作负载受害者的工作负载，并确定这些相同的工作负载何时成为欺凌工作负载。工作负载可能会欺凌自身。例如，受策略组限制所限制的高性能工作负载会导致策略组中的所有工作负载（包括其自身）受到限制。在持续发生的性能事件中，作为欺凌者或受害者的工作负载可能会更改其角色，或者不再是该事件的参与者。

管理性能阈值

在 **Active IQ Unified Manager** 中管理性能阈值

性能阈值策略使您能够确定 Unified Manager 生成事件的时间点，以告知系统管理员可能影响工作负载性能的问题。这些阈值策略称为 用户定义 性能阈值。

此版本支持用户定义、系统定义和动态性能阈值。使用动态和系统定义的性能阈值，Unified Manager 分析工作负载活动以确定适当的阈值。使用用户定义的阈值，您可以为许多性能计数器和许多存储对象定义性能上限。

系统定义的性能阈值和动态性能阈值由 Unified Manager 设置，不可配置。如果从任何系统定义的性能阈值策略接收到不必要的事件，则可以从“事件设置”页面禁用单个策略。

在 **Active IQ Unified Manager** 中使用用户定义的性能阈值策略

您可以为存储对象（例如，聚合和卷）设置性能阈值策略，以便将事件发送给存储管理员，以通知管理员群集遇到性能问题。

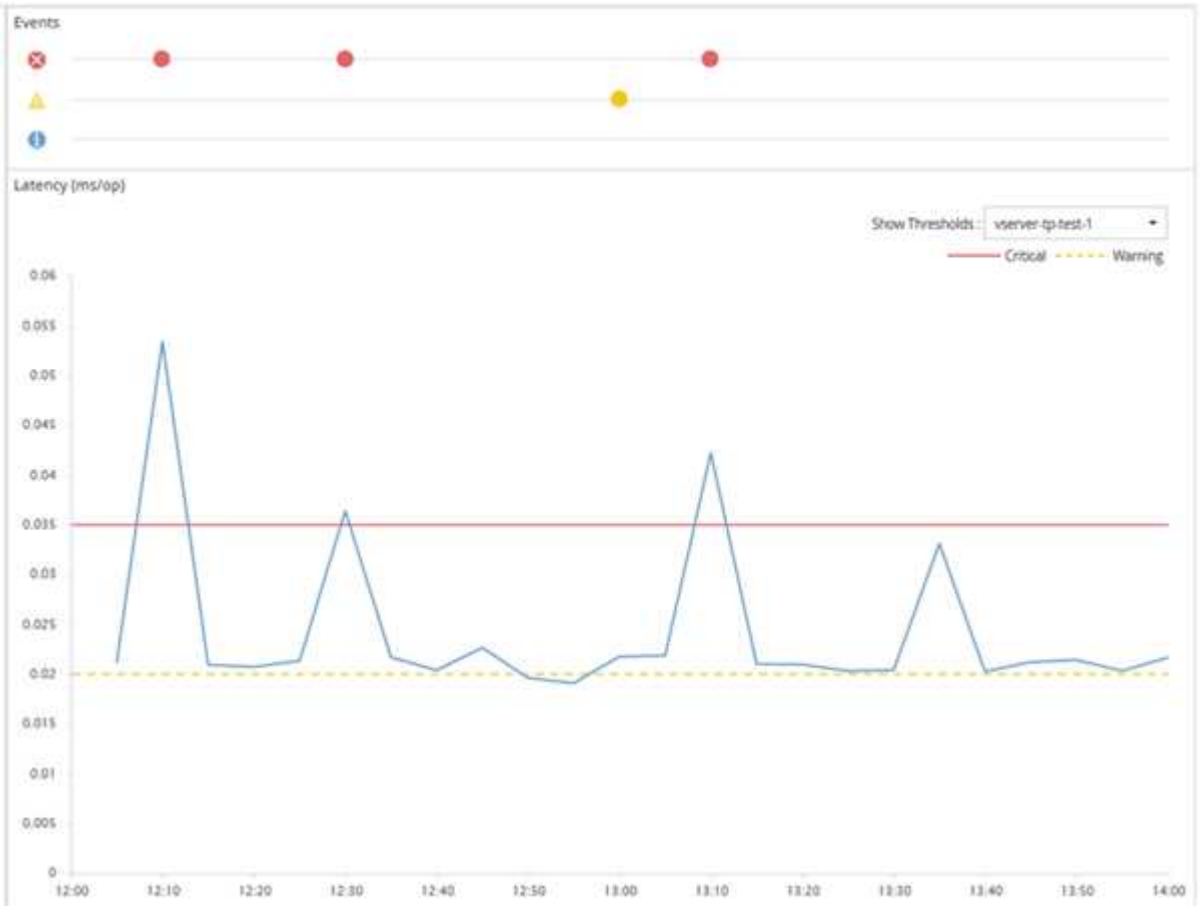
您可以通过以下方式为存储对象创建性能阈值策略：

- 选择存储对象
- 选择与该对象关联的性能计数器
- 指定用于定义性能计数器上限的值，这些上限被视为警告和严重情况
- 指定一个时间段，该时间段定义计数器必须超过上限的时间长度

例如，您可以对卷设置性能阈值策略，以便在该卷的 IOPS 连续 10 分钟超过每秒 750 次操作时收到关键事件通知。此相同的阈值策略还可以指定在 IOPS 超过每秒 500 次操作达 10 分钟时发送警告事件。

当前版本提供在计数器值超过阈值设置时发送事件的阈值。您不能设置计数器值低于阈值设置时发送事件的阈值。

此处显示了一个计数器图表示例，表明在 1:00 时突破了警告阈值（黄色图标），在 12:10、12:30 和 1:10 时突破了临界阈值（红色图标）：



阈值违规必须在指定的持续时间内持续发生。如果阈值因任何原因低于限值，则后续违规被视为新持续时间的开始。

某些群集对象和性能计数器使您能够创建组合阈值策略，该策略要求两个性能计数器在生成事件之前超过其最大限制。例如，您可以使用以下条件创建阈值策略：

集群对象	性能计数器	警告阈值	严重阈值	持续时间
卷	延迟	10 毫秒	20 毫秒	15 分钟
聚合	利用率	65%	85%	

使用两个集群对象的阈值策略仅在违反这两个条件时才会生成事件。例如，使用表中定义的阈值策略：

如果卷延迟平均为.....	而且聚合磁盘利用率为.....	操作
15 毫秒	50%	未报告任何事件。
15 毫秒	75%	已报告警告事件。
25 毫秒	75%	已报告警告事件。
25 毫秒	90%	已报告严重事件。

响应 **Active IQ Unified Manager** 中违反性能阈值策略的问题

当计数器值超过其定义的性能阈值的时间达到持续时间中指定的时间量时，将违反该阈值并报告事件。

事件会导致启动以下操作：

- 此事件显示在“仪表板”、“性能群集摘要”页、“事件”页和特定于对象的“性能清单”页中。
- （可选）有关事件的电子邮件警报可以发送到一个或多个电子邮件收件人，SNMP 陷阱可以发送到陷阱接收器。
- （可选）可以执行脚本来自动修改或更新存储对象。

始终执行第一个操作。您可以在警报设置页面中配置是否执行可选操作。您可以根据是否违反警告或严重阈值策略来定义唯一操作。

在存储对象上发生性能阈值策略违规后，不会为该策略生成进一步的事件，直到计数器值低于阈值，此时为该限制重置持续时间。在继续超出阈值的同时，会不断更新事件的结束时间，以反映此事件正在进行中。

阈值事件捕获或冻结与严重性和策略定义相关的信息，以便即使将来修改了阈值策略，也会随事件显示唯一的阈值信息。

了解使用 **Active IQ Unified Manager** 中的阈值跟踪的性能计数器

某些常见性能计数器（如 IOPS 和 MB/s）可以为所有存储对象设置阈值。还有其他计数器只能为某些存储对象设置阈值。

可用性能计数器

存储对象	性能计数器	问题描述
集群	IOPS	集群每秒处理的平均输入/输出操作数。
MB/秒	每秒传入和传出此集群的平均数据兆字节数。	节点
IOPS	节点每秒处理的平均输入/输出操作数。	MB/秒
每秒传入和传出此节点的数据的平均 MB 数。	延迟	节点响应应用程序请求所需的平均毫秒数。
利用率	正在使用的节点 CPU 和 RAM 的平均百分比。	已用性能容量
节点正在消耗的性能容量的平均百分比。	已用性能容量 - 接管	节点正在消耗的性能容量的平均百分比，加上其配对节点的性能容量。
聚合	IOPS	聚合每秒处理的平均输入/输出操作数。
MB/秒	每秒传入和传出此聚合的平均数据兆字节数。	延迟
聚合响应应用程序请求所需的平均毫秒数。	利用率	正在使用的聚合磁盘的平均百分比。
已用性能容量	聚合正在消耗的性能容量的平均百分比。	Storage VM
IOPS	SVM 每秒处理的平均输入/输出操作数。	MB/秒
每秒传入和传出此 SVM 的平均数据兆字节数。	延迟	SVM 响应应用程序请求所需的平均毫秒数。
卷	IOPS	卷每秒处理的平均输入/输出操作数。
MB/秒	每秒传入和传出此卷的平均数据兆字节数。	延迟
卷响应应用程序请求所需的平均毫秒数。	缓存未命中率	从卷返回而不是从缓存返回的来自客户端应用程序的读取请求的平均百分比。
LUN	IOPS	LUN 每秒处理的平均输入/输出操作数。
MB/秒	每秒与此 LUN 之间传输的平均数据量（以兆字节为单位）。	延迟
LUN 响应应用程序请求所用的平均毫秒数。	命名空间	IOPS
命名空间每秒处理的平均输入/输出操作数。	MB/秒	每秒传输到此命名空间和从此命名空间传输的平均数据 MB 数。

存储对象	性能计数器	问题描述
延迟	命名空间响应应用程序请求所需的平均毫秒数。	端口
带宽利用率	当前正在使用的端口可用带宽的平均百分比。	MB/秒
每秒传入和传出此端口的平均数据兆字节数。	网络接口（LIF）	MB/秒

了解 **Active IQ Unified Manager** 中的组合阈值策略对象和计数器

组合策略中只能同时使用某些性能计数器。当指定主性能计数器和辅助性能计数器时，在生成事件之前，两个性能计数器都必须超过其最大限制。

主存储对象和计数器	辅助存储对象和计数器
卷延迟	卷 IOPS
卷 MB/s	聚合利用率
聚合已用性能容量	节点利用率
已用节点性能容量	已用节点性能容量 - 接管
LUN 延迟	LUN IOPS
LUN MB/s	聚合利用率
聚合已用性能容量	节点利用率
已用节点性能容量	已用节点性能容量 - 接管

将卷组合策略应用于 FlexGroup 卷而不是 FlexVol 卷时，只能选择“`Volume IOPS`”和“`Volume MB/s`”属性作为辅助计数器。如果阈值策略包含节点或聚合属性之一，则该策略将不会应用于 FlexGroup 卷，并且您将收到描述此情况的错误消息。这是因为 FlexGroup 卷可以存在于多个节点或聚合上。

在 **Active IQ Unified Manager** 中创建用户定义的性能阈值策略

您可以为存储对象创建性能阈值策略，以便在性能计数器超过特定值时发送通知。事件通知表明集群遇到性能问题。

开始之前

您必须具有应用程序管理员角色。

您可以在"Create Performance Threshold Policy"页面上输入阈值来创建性能阈值策略。您可以通过在此页面上定义所有策略值来创建新策略，也可以复制现有策略并更改副本中的值（称为_克隆_）。

数字的有效阈值为 0.001 至 10,000,000，百分比的有效阈值为 0.001-100，已用性能容量百分比的有效阈值为 0.001-200。

当前版本提供在计数器值超过阈值设置时发送事件的阈值。您不能设置计数器值低于阈值设置时

发送事件的阈值。

步骤

1. 在左侧导航窗格中，选择*事件阈值* > 性能。

   此时将显示性能阈值页面。

2. 根据您是要创建新策略，还是要克隆类似策略并修改克隆版本，单击相应的按钮。

目的	单击.....
创建新策略	创建
克隆现有策略	选择现有策略并单击*克隆*

   此时将显示“创建性能阈值策略”页面或“克隆性能阈值策略”页面。

3. 通过指定要为特定存储对象设置的性能计数器阈值来定义阈值策略：

   a. 选择存储对象类型并指定策略的名称和描述。

   b. 选择要跟踪的性能计数器，并指定定义“警告”和“严重”事件的限制值。

      必须至少定义一个警告或一个严重限制。无需同时定义两种类型的限制。

   c. 如果需要，请选择辅助性能计数器，并指定警告和严重事件的限制值。

      包含辅助计数器要求在超出阈值并报告事件之前，两个计数器都必须超过限制值。只能使用组合策略配置某些对象和计数器。

   d. 选择必须突破限制值才能发送事件的持续时间。

   克隆现有策略时，必须为策略输入一个新名称。

4. 单击 **Save** 保存策略。

   您将返回到“性能阈值”页面。页面顶端的成功消息确认阈值策略已创建，并提供指向此对象类型的清单页面的链接，以便您可以立即将新策略应用于存储对象。

如果此时要将新的阈值策略应用于存储对象，可以单击 立即转到 **object_type** 链接转到清单页面。

在 **Active IQ Unified Manager** 中为存储对象分配性能阈值策略

将用户定义的性能阈值策略分配给存储对象，以便 Unified Manager 在性能计数器的值超过策略设置时报告事件。

开始之前

您必须具有应用程序管理员角色。

要应用于对象的性能阈值策略必须存在。

一次只能将一个性能策略应用于一个对象或一组对象。

您最多可以为每个存储对象分配三个阈值策略。在为多个对象分配策略时，如果任何对象已分配了最大数量的策略，则 Unified Manager 将执行以下操作：

- 将策略应用于未达到最大值的所有选定对象
- 忽略已达到策略最大数量的对象
- 显示一条消息，指出未将策略分配给所有对象

步骤

1. 从任何存储对象的性能清单页面中，选择要向其分配阈值策略的对象：

要将阈值分配给……	单击……
单个对象	该对象左侧的复选框。
多个对象	每个对象左侧的复选框。
页面上的所有对象	下拉框，然后选择*选择此页面上的所有对象*。
所有相同类型的对象	下拉框，然后选择*选择所有对象*。

   您可以使用排序和筛选功能来优化清单页面上的对象列表，以便更轻松地将阈值策略应用于许多对象。

2. 进行选择，然后单击*分配性能阈值策略*。

   此时将显示分配性能阈值策略页面，其中显示针对该特定类型存储对象的阈值策略列表。

3. 单击每个策略可显示性能阈值设置的详细信息，以验证您选择的阈值策略是否正确。
4. 选择适当的阈值策略后，单击*分配策略*。

   页面顶端的一条成功消息可确认已将阈值策略分配给一个或多个对象，并提供指向“警报”页面的链接，以便您可以为此对象和策略配置警报设置。

如果希望通过电子邮件或 SNMP 陷阱发送警报，以通知您已生成特定的性能事件，则必须在“警报设置”页面中配置警报设置。

在 **Active IQ Unified Manager** 中查看性能阈值策略

您可以从“性能阈值”页面查看所有当前定义的性能阈值策略。

阈值策略列表按策略名称的字母顺序排序，其中包括所有类型的存储对象的策略。您可以单击列标题，按该列对策略进行排序。如果要查找特定策略，请使用筛选器和搜索机制来优化清单列表中显示的阈值策略列表。

您可以将光标悬停在策略名称和条件名称上，以查看策略的配置详细信息。此外，您可以使用提供的按钮创建、克隆、编辑和删除用户定义的阈值策略。

步骤

1. 在左侧导航窗格中，选择*事件阈值* > 性能。

   此时将显示性能阈值页面。

在 **Active IQ Unified Manager** 中编辑用户定义的性能阈值策略

您可以编辑现有性能阈值策略的阈值设置。如果您发现在某些阈值条件下收到的警报太多或太少，这可能会很有用。

开始之前

您必须具有应用程序管理员角色。

对于现有的阈值策略，无法更改策略名称或受监控的存储对象类型。

步骤

1. 在左侧导航窗格中，选择*事件阈值* > 性能。

   将显示性能阈值页面。

2. 选择要更改的阈值策略，然后单击*编辑*。

   此时将显示编辑性能阈值策略页面。

3. 对阈值策略进行更改，然后单击*保存*。

   此时将返回“性能阈值”页面。

保存后，更改将立即更新到使用该策略的所有存储对象。

根据您对策略所做更改的类型，您可能需要在"警报设置"页面中查看使用该策略的对象所配置的警报设置。

从 **Active IQ Unified Manager** 中的存储对象删除性能阈值策略

当您不再希望 Unified Manager 监视性能计数器的值时，可以从存储对象中删除用户定义的性能阈值策略。

开始之前

您必须具有应用程序管理员角色。

一次只能从所选对象中删除一个策略。

您可以通过在列表中选择多个对象来从多个存储对象中删除阈值策略。

步骤

1. 从任何存储对象的*清单*页面中，选择至少应用了一个性能阈值策略的一个或多个对象。

要从……清除阈值	操作
单个对象	选中该对象左侧的复选框。
多个对象	选中每个对象左侧的复选框。
页面上的所有对象	单击列标题中的  。

2. 单击 清除性能阈值策略。

此时将显示“清除阈值策略”页面，其中显示当前分配给存储对象的阈值策略列表。

3. 选择要从对象中删除的阈值策略，然后单击*清除策略*。

   选择阈值策略时，将显示策略的详细信息，以便确认已选择适当的策略。

了解 Active IQ Unified Manager 中的性能阈值策略更改

如果调整现有性能阈值策略的计数器值或持续时间，策略更改将应用于使用该策略的所有存储对象。新设置将立即生效，Unified Manager 将开始将性能计数器值与所有新收集的性能数据的新阈值设置进行比较。

如果使用更改的阈值策略的对象存在任何活动事件，则这些事件将被标记为已过时，并且阈值策略将作为新定义的阈值策略开始监控计数器。

在计数器图表详细视图中查看已应用阈值的计数器时，临界和警告阈值线反映当前阈值设置。即使在旧阈值设置生效时查看历史数据，原始阈值设置也不会显示在此页面上。

由于旧的阈值设置不会显示在计数器图表详细视图中，因此您可能会看到显示在当前阈值线下方的历史事件。

在 Active IQ Unified Manager 中移动对象时管理阈值策略

由于性能阈值策略已分配给存储对象，因此如果移动对象，则所有分配的阈值策略在移动完成后仍会附加到对象。例如，如果将卷或 LUN 移动到其他聚合，则新聚合上的卷或 LUN 的阈值策略仍处于活动状态。

如果阈值策略（组合策略）存在辅助计数器条件（例如，如果其他条件分配给聚合或节点），则辅助计数器条件将应用于卷或 LUN 已移动到的新聚合或节点。

如果使用更改的阈值策略的对象存在任何新的活动事件，则这些事件将被标记为已过时，并且阈值策略将作为新定义的阈值策略开始监视计数器。

卷移动操作导致 ONTAP 发送信息更改事件。更改事件图标显示在“性能资源管理器”页面和“工作负载分析”页面上的“事件时间表”中，以指示移动操作完成的时间。

如果将对象移动到其他群集，则会从对象中删除用户定义的阈值策略。如果需要，必须在移动操作完成后为对象分配阈值策略。但是，动态和系统定义的阈值策略会在对象移动到新群集后自动应用于该对象。

HA 接管和交还期间的阈值策略功能

当在高可用性（HA）配置中发生接管或交回操作时，从一个节点移动到另一个节点的对象将以与手动移动操作相同的方式保留其阈值策略。由于 Unified Manager 每 15 分钟检查一次集群配置的更改，因此在下次轮询集群配置之前，不会确定切换到新节点的影响。

如果接管和交还操作都在 15 分钟的配置更改收集期内发生，您可能看不到性能统计数据从一个节点移动到另一个节点。

聚合重新定位期间的阈值策略功能

如果使用 `aggregate relocation start` 命令将聚合从一个节点移动到另一个节点，则所有对象都将保留单个阈值策略和组合阈值策略，并将阈值策略的节点部分应用于新节点。

MetroCluster 切换期间的阈值策略功能

在 MetroCluster 配置中从一个集群移动到另一个集群的对象不会保留其用户定义的阈值策略设置。如果需要，您可以在已移动到配对集群的卷和 LUN 上应用阈值策略。在对象移回其原始集群后，将自动重新应用用户定义的阈值策略。

有关信息，请参见 "切换和切回期间的卷行为"。

分析性能事件

分析 **Active IQ Unified Manager** 中的性能事件

您可以分析性能事件以确定它们何时被检测到，它们是活动的（新的还是已确认的）还是过时的，涉及的工作负载和集群组件，以及用于自行解决事件的选项。

在 **Active IQ Unified Manager** 中显示性能事件信息

您可以使用事件管理清单页面查看由 Unified Manager 监控的集群上的所有性能事件列表。通过查看此信息，您可以确定最关键的事件，然后深入查看详细信息以确定事件的原因。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。

事件列表按检测时间排序，最近的事件列在前面。您可以单击列标题，根据该列对事件进行排序。例如，您可以按“状态”列进行排序，以按严重程度查看事件。如果您正在查找特定事件或特定类型的事件，则可以使用筛选器和搜索机制来优化列表中显示的事件列表。

所有来源的事件都显示在此页面上：

- 用户定义的性能阈值策略
- 系统定义的性能阈值策略
- 动态性能阈值

“事件类型”列列出了事件的来源。您可以选择一个事件，在“事件详细信息”页面中查看有关该事件的详细信息。

步骤

1. 在左侧导航窗格中，单击*事件管理*。
2. 在“视图”菜单中，选择 活动性能事件。

   该页面显示过去 7 天内生成的所有“新建”和“已确认”性能事件。

3. 找到要分析的事件，然后单击该事件名称。

此时将显示此事件的详细信息页面。

> 您也可以通过单击 Performance Explorer 页面中的事件名称链接或警报电子邮件中的链接来显示事件的详细信息页面。

分析用户定义的性能阈值事件

分析 **Active IQ Unified Manager** 中用户定义的性能阈值产生的事件

从用户定义的阈值生成的事件指示特定存储对象（例如聚合或卷）的性能计数器已超过您在策略中定义的阈值。这表示集群对象遇到性能问题。

您可以使用“事件详细信息”页面分析性能事件，并在必要时采取纠正措施，使性能恢复正常。

在 **Active IQ Unified Manager** 中响应用户定义的性能阈值事件

您可以使用 Unified Manager 调查由性能计数器超出用户定义的警告或严重阈值引起的性能事件。您还可以使用 Unified Manager 检查集群组件的运行状况，以查看在组件上检测到的近期运行状况事件是否导致了性能事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须有新的或过时的性能事件。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看*描述*，其中描述了导致此事件的阈值违规行为。

   例如，消息 “Latency value of 456 ms/op has triggered a WARNING event based on threshold setting of 400 ms/op” 表示该对象发生了延迟警告事件。

3. 将光标悬停在策略名称上，以显示有关触发此事件的阈值策略的详细信息。

   这包括策略名称、正在评估的性能计数器、必须突破才能被视为严重或警告事件的计数器值，以及计数器必须超过该值的持续时间。

4. 记下*事件触发时间*，以便调查是否有其他事件在同一时间发生，从而可能对此事件产生影响。
5. 按照以下选项之一进一步调查事件，以确定是否需要执行任何操作来解决性能问题：

选项	可能的调查操作
单击源对象名称以显示该对象的“资源管理器”页面。	通过此页面，您可以查看对象详细信息，并将此对象与其他类似的存储对象进行比较，以查看其他存储对象是否大约在同一时间存在性能问题。例如，查看同一聚合中的其他卷是否也存在性能问题。
单击集群名称以显示“集群摘要”页面。	通过此页面，您可以查看此对象所在集群的详细信息，以了解大约在同一时间是否发生了其他性能问题。

分析系统定义的性能阈值事件

分析 **Active IQ Unified Manager** 中系统定义的性能阈值事件

系统定义的性能阈值生成的事件指示特定存储对象的性能计数器或性能计数器集已超过系统定义策略的阈值。这表示存储对象（例如聚合或节点）遇到性能问题。

您可以使用“事件详细信息”页面分析性能事件，并在必要时采取纠正措施，使性能恢复正常。

Cloud Volumes ONTAP、ONTAP Edge 或 ONTAP Select 系统上未启用系统定义的阈值策略。

响应 **Active IQ Unified Manager** 中系统定义的性能阈值事件

您可以使用 Unified Manager 调查性能计数器超出系统定义的警告阈值引起的性能事件。您还可以使用 Unified Manager 检查集群组件的运行状况，以查看在组件上检测到的最近事件是否导致了性能事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须有新的或过时的性能事件。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看*描述*，其中描述了导致此事件的阈值违规行为。

   例如，消息 “Node utilization value of 90 % has triggered a WARNING event based on threshold setting of 85 %” 表示集群对象发生了节点利用率警告事件。

3. 记下*事件触发时间*，以便调查是否有其他事件在同一时间发生，从而可能对此事件产生影响。
4. 在*系统诊断*下，查看系统定义策略对集群对象执行的分析类型的简要说明。

   对于某些事件，诊断旁边会显示绿色或红色图标，以指示在该特定诊断中是否发现了问题。对于其他类型的系统定义事件，计数器图表显示对象的性能。

5. 在*建议操作*下，单击*帮助我执行此操作*链接以查看您可以执行的建议操作，尝试自行解决性能事件。

响应 **Active IQ Unified Manager** 中的 **QoS** 策略组性能事件

当工作负载吞吐量（IOPS、IOPS/TB或MBps）超过定义的ONTAP QoS策略设置且工作负载延迟受到影响时，Unified Manager会生成QoS策略警告事件。这些系统定义的事件提供了在许多工作负载受延迟影响之前纠正潜在性能问题的机会。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须存在新的、已确认的或已过时的性能事件。

当工作负载吞吐量在前一小时的每个性能收集期间超过定义的 QoS 策略设置时，Unified Manager 会生成 QoS

策略违规的警告事件。在每个收集期间，工作负载吞吐量可能仅在短时间内超过 QoS 阈值，但 Unified Manager 仅在图表上显示收集期间的“average”吞吐量。因此，即使工作负载的吞吐量可能未超过图表中显示的策略阈值，您也可能会收到 QoS 事件。

您可以使用 System Manager 或 ONTAP 命令来管理策略组，包括以下任务：

- 为工作负载创建新策略组
- 在策略组中添加或删除工作负载
- 在策略组之间移动工作负载
- 更改策略组的吞吐量限制
- 将工作负载移动到其他聚合或节点

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看*描述*，其中描述了导致此事件的阈值违规行为。

   例如，消息 “vol1_NFS1 上的 IOPS 值为 1,352 IOPS 已触发 WARNING 事件以确定工作负载的潜在性能问题” 表示卷 vol1_NFS1 上发生了 QoS 最大 IOPS 事件。

3. 查看*事件信息*部分，了解有关事件发生时间以及事件处于活动状态多长时间的更多详细信息。

   此外，对于共享 QoS 策略吞吐量的卷或 LUN，您可以看到消耗最多 IOPS 或 MBps 的前三个工作负载的名称。

4. 在 系统诊断 部分下，查看两个图表：一个用于总平均 IOPS 或 MBps（取决于事件），另一个用于延迟。通过这种排列方式，您可以看到当工作负载接近 QoS 最大限制时，哪些集群组件对延迟的影响最大。

   对于共享 QoS 策略事件，吞吐量图表中会显示前三个工作负载。如果共享 QoS 策略的工作负载超过三个，则其他工作负载将汇总至"`Other workloads`"类别。此外，延迟图表会显示 QoS 策略中所有工作负载的平均延迟。

   请注意，对于自适应 QoS 策略事件，IOPS 和 MBps 图表显示 ONTAP 已根据卷大小从分配的 IOPS/TB 阈值策略转换的 IOPS 或 MBps 值。

5. 在*建议操作*部分下，查看建议并确定应执行哪些操作以避免工作负载的延迟增加。

   如果需要，请单击 帮助 按钮以查看有关您可以执行的建议操作的更多详细信息，以尝试解决性能事件。

了解 **Active IQ Unified Manager** 中具有已定义块大小的自适应 **QoS** 事件

自适应 QoS 策略组会根据卷大小自动缩放吞吐量上限或下限，并随着卷大小的变化保持 IOPS 与 TB 的比例。从 ONTAP 9.5 开始，您可以在 QoS 策略中指定块大小，以同时有效地应用 MB/s 阈值。

在自适应 QoS 策略中分配 IOPS 阈值仅对每个工作负载中发生的操作数量设置限制。根据在生成工作负载的客户端上设置的块大小，某些 IOPS 包含更多数据，因此会给处理操作的节点带来更大的负担。

使用以下公式生成工作负载的 MB/s 值：

```
MB/s = (IOPS * Block Size) / 1000
```

如果工作负载平均为 3,000 IOPS，并且客户端上的块大小设置为 32 KB，则此工作负载的有效 MB/s 为 96。如果相同的工作负载平均为 3,000 IOPS，并且客户端上的块大小设置为 48 KB，则此工作负载的有效 MB/s 为 144。可以看到，当块大小较大时，节点处理的数据量增加了 50%。

让我们看一下以下具有定义块大小的自适应 QoS 策略，以及如何根据客户端上设置的块大小触发事件。

创建策略并将峰值吞吐量设置为 2,500 IOPS/TB，块大小为 32KB。这有效地将已用容量为 1 TB 的卷的 MB/s 阈值设置为 80 MB/s（（2500 IOPS * 32KB）/ 1000）。请注意，当吞吐量值比定义的阈值低 10% 时，Unified Manager 会生成警告事件。事件在以下情况下生成：

已用容量	当吞吐量超过此数量时生成事件.....	
	IOPS	MB/秒
1 TB	2,250 IOPS	72 MB/s
2 TB	4,500 IOPS	144 MB/s
5 TB	11,250 IOPS	360 MB/s

如果卷使用 2TB 的可用空间，并且 IOPS 为 4,000，并且客户端上的 QoS 块大小设置为 32KB，则 MB/ps 吞吐量为 128 MB/s（（4,000 IOPS * 32 KB）/ 1000）。在此方案中不会生成任何事件，因为 4,000 IOPS 和 128 MB/s 均低于使用 2 TB 空间的卷的阈值。

如果卷正在使用可用空间中的 2TB，IOPS 为 4,000，且客户端上的 QoS 块大小设置为 64KB，则 MB/s 吞吐量为 256 MB/s （（4,000 IOPS * 64 KB）/ 1000）。在这种情况下，4,000 IOPS 不会生成事件，但 256 MB/s 的 MB/s 值超过了 144 MB/s 的阈值，因此会生成事件。

因此，当基于包含块大小的自适应 QoS 策略的 MB/s 违规触发事件时，“事件详细信息”页面的“系统诊断”部分中将显示 MB/s 图表。如果基于自适应 QoS 策略的 IOPS 违规触发事件，则在“系统诊断”部分显示 IOPS 图表。如果 IOPS 和 MB/s 都发生违规，您将收到两个事件。

有关调整 QoS 设置的更多信息，请参见 "性能管理概述"。

响应 **Active IQ Unified Manager** 中的节点资源过度利用事件

当单个节点运行超出其运行效率的界限，从而可能影响工作负载延迟时，Unified Manager 会生成节点资源过度使用的警告事件。这些系统定义的事件提供了在许多工作负载受到延迟影响之前纠正潜在性能问题的机会。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须有新的或过时的性能事件。

Unified Manager 通过查找使用超过 100% 性能容量超过 30 分钟的节点，为节点资源过度使用策略违规生成警告事件。

您可以使用 System Manager 或 ONTAP 命令来更正此类型的性能问题，包括以下任务：

- 创建 QoS 策略并将其应用于任何过度使用系统资源的卷或 LUN
- 降低已应用工作负载的策略组的 QoS 最大吞吐量限制
- 将工作负载移动到其他聚合或节点
- 通过向节点添加磁盘或升级为 CPU 更快且 RAM 更大的节点来提高容量

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看*描述*，其中描述了导致此事件的阈值违规行为。

   例如，消息 “Perf.simplicity-02 上的 Capacity Used 值为 139%，已触发 WARNING 事件以确定 Data Processing 单元中的潜在性能问题。” 表示节点 simplicity-02 上的性能容量被过度使用并影响节点性能。

3. 在*系统诊断*部分下，查看三个图表：一个用于节点上使用的性能容量，一个用于顶级工作负载使用的平均存储 IOPS，一个用于顶级工作负载上的延迟。以这种方式排列时，您可以查看哪些工作负载是节点上延迟的原因。

   您可以通过将光标移到 IOPS 图表上来查看哪些工作负载应用了 QoS 策略，哪些未应用 QoS 策略。

4. 在*建议操作*部分下，查看建议并确定应执行哪些操作以避免工作负载的延迟增加。

   如果需要，请单击 帮助 按钮以查看有关您可以执行的建议操作的更多详细信息，以尝试解决性能事件。

响应 **Active IQ Unified Manager** 中的集群不平衡性能事件

当群集中的一个节点以比其他节点高得多的负载运行时，Unified Manager 将生成群集不平衡警告事件，因此可能会影响工作负载延迟。这些系统定义的事件提供了在许多工作负载受到延迟影响之前纠正潜在性能问题的机会。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

Unified Manager 通过比较集群中所有节点的性能容量使用值，以查看任何节点之间是否存在 30% 的负载差异，从而为集群不平衡阈值策略违规生成警告事件。

这些步骤可帮助您确定以下资源，以便将高性能工作负载移动到利用率较低的节点：

- 同一集群上利用率较低的节点
- 新节点上利用率最低的聚合
- 当前节点上性能最高的卷

步骤

1. 显示*事件*详细信息页面以查看有关事件的信息。
2. 查看*描述*，其中描述了导致此事件的阈值违规行为。

   例如，消息“已用性能容量计数器表示集群 `Dallas-1-8` 中节点之间存在 `62%` 的负载差异，并已根据系统阈值 `30%` 触发警告事件”表示其中一个节点上的性能容量被过度使用并影响节点性能。

3. 查看 **Suggested Actions** 中的文本，以将高性能卷从性能容量使用值较高的节点移至性能容量使用值最低的节点。
4. 识别具有最高和最低性能容量使用值的节点：
   a. 在*事件信息*部分，单击源集群的名称。
   b. 在*集群/性能摘要*页面中，单击*托管对象*区域中的*节点*。
   c. 在*节点*清单页面中，按*已用性能容量*列对节点进行排序。
   d. 确定性能容量使用值最高和最低的节点，并记录这些节点的名称。
5. 确定在具有最高性能容量使用值的节点上使用最多 IOPS 的卷：
   a. 单击具有最高性能容量使用值的节点。
   b. 在*节点/性能资源管理器*页面中，从*查看和比较*菜单中选择*此节点上的聚合*。
   c. 单击具有最高性能容量使用值的聚合。
   d. 在*聚合/性能资源管理器*页面中，从*查看和比较*菜单中选择*此聚合上的卷*。
   e. 按 **IOPS** 列对卷进行排序，并记下使用最多 IOPS 的卷的名称，以及该卷所在聚合的名称。
6. 识别性能容量使用值最低的节点上利用率最低的聚合：
   a. 单击*存储* > *聚合*以显示*聚合*清单页面。
   b. 选择*性能：所有聚合*视图。
   c. 单击 过滤器 按钮并添加一个过滤器，其中 “Node” 等于您在步骤 4 中记下的已用性能容量值最低的节点的名称。
   d. 写下性能容量使用值最低的聚合的名称。
7. 将卷从过载节点移动到您确定在新节点上利用率较低的聚合。

   您可以使用 ONTAP System Manager、OnCommand Workflow Automation、ONTAP 命令或这些工具的组合来执行移动操作。

几天后，请检查您是否从此集群接收到相同的集群不平衡事件。

分析动态性能阈值事件

分析 **Active IQ Unified Manager** 中动态性能阈值的事件

由动态阈值生成的事件表明，与预期响应时间范围相比，工作负载的实际响应时间（延迟）过高或过低。您可以使用“事件详细信息”页面分析性能事件，并在必要时采取纠正措施，使性能恢复正常。

在 Cloud Volumes ONTAP、ONTAP Edge 或 ONTAP Select 系统上未启用动态性能阈值。

在 **Active IQ Unified Manager** 中识别动态性能事件中的受害工作负载

在 Unified Manager 中，您可以识别哪些卷工作负载的响应时间（延迟）偏差最大，这是由争用中的存储组件引起的。识别这些工作负载有助于您了解为什么访问它们的客户端应用程序的执行速度比平时慢。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须有新的、已确认的或过时的动态性能事件。

“事件详细信息”页面显示用户定义和系统定义工作负载的列表，按组件上活动或使用情况的最大偏差或受事件影响最大进行排名。这些值基于 Unified Manager 在检测到并上次分析事件时识别的峰值。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 在 Workload Latency 和 Workload Activity 图表中，选择 **Victim Workloads**。
3. 将光标悬停在图表上，以查看影响组件的主要用户定义工作负载以及受害者工作负载的名称。

在 **Active IQ Unified Manager** 中识别动态性能事件中的欺凌工作负载

在 Unified Manager 中，您可以识别哪些工作负载对处于争用状态的集群组件的使用量偏差最大。识别这些工作负载有助于您了解集群中某些卷的响应时间（延迟）较慢的原因。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须有新的、已确认的或过时的动态性能事件。

“事件详细信息”页面显示用户定义和系统定义的工作负载列表，这些工作负载按组件的最高使用率或受事件影响最大的程度进行排序。这些值基于 Unified Manager 在检测到并上次分析事件时识别的峰值。

步骤

1. 显示事件详细信息页面以查看有关事件的信息。
2. 在 Workload Latency 和 Workload Activity 图表中，选择 **Bully Workloads**。
3. 将光标悬停在图表上以查看影响组件的排名靠前的用户定义恶霸工作负载。

在 **Active IQ Unified Manager** 中识别动态性能事件中的鲨鱼工作负载

在 Unified Manager 中，您可以识别哪些工作负载在争用中的存储组件的使用率偏差最大。识别这些工作负载可帮助您确定是否应将这些工作负载迁移到利用率较低的集群。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 有新的、已确认的或过时的性能动态事件。

“事件详细信息”页面显示用户定义和系统定义的工作负载列表，这些工作负载按组件的最高使用率或受事件影响最大的程度进行排序。这些值基于 Unified Manager 在检测到并上次分析事件时识别的峰值。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 在 Workload Latency 和 Workload Activity 图表中，选择 **Shark Workloads**。
3. 将光标悬停在图表上，以查看影响组件的顶级用户定义的工作负载以及 shark 工作负载的名称。

MetroCluster 配置的性能事件分析

使用 Active IQ Unified Manager 分析 MetroCluster 性能事件

您可以使用 Unified Manager 分析 MetroCluster 配置的性能事件。您可以识别此事件所涉及的工作负载，并查看解决此问题的建议措施。

MetroCluster 性能事件可能是由于 *bully* workloads 过度使用群集之间的交换机间链路（ISL），或是由于链路运行状况问题。Unified Manager 独立监控 MetroCluster 配置中的每个群集，而不考虑伙伴群集上的性能事件。

MetroCluster 配置中两个集群的性能事件也会显示在 Unified Manager 仪表板页面上。您还可以查看 Unified Manager 的运行状况页面，以检查每个集群的运行状况并查看其关系。

在 Active IQ Unified Manager 中的集群上分析 MetroCluster 性能事件

您可以使用 Unified Manager 在检测到性能事件的 MetroCluster 配置中分析集群。您可以确定集群名称、事件检测时间以及所涉及的 *bully* 和 *victim* 工作负载。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- MetroCluster 配置必须有新的、已确认的或过时的性能事件。
- MetroCluster 配置中的两个集群必须由同一个 Unified Manager 实例监控。

步骤

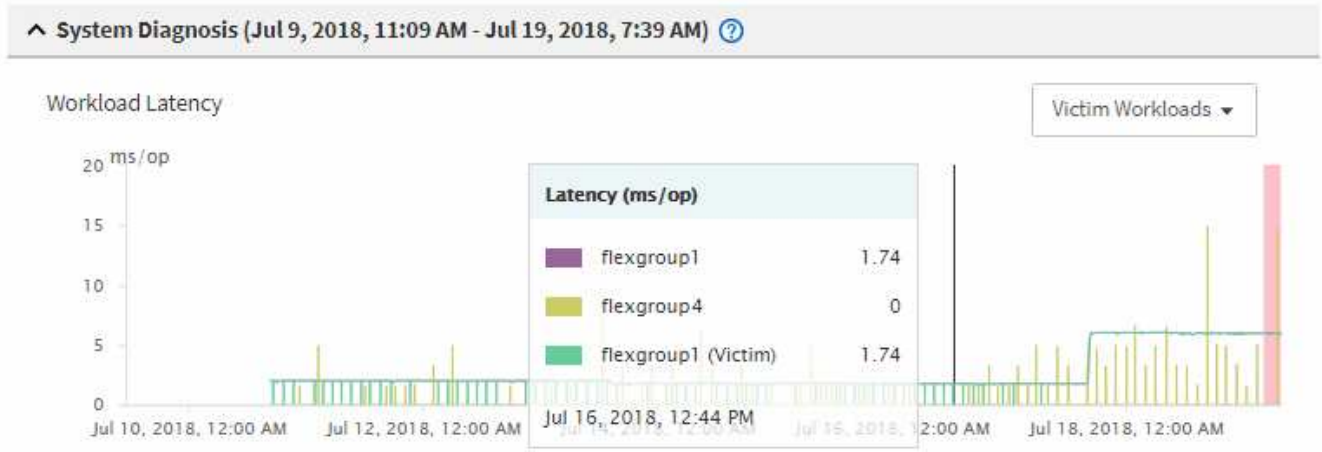
1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 查看事件描述，了解所涉及的工作负载名称以及所涉及的工作负载数量。

   在此示例中，“MetroCluster 资源”图标为红色，表示 MetroCluster 资源处于争用状态。将光标定位在图标上以显示图标的说明。



3. 记下集群名称和事件检测时间，您可以使用这些信息来分析配对集群上的性能事件。
4. 在图表中，查看 *victim* 工作负载，以确认其响应时间高于性能阈值。

   在此示例中，受害者工作负载显示在悬停文本中。延迟图表在较高层面上显示了所涉及的受害者工作负载的一致延迟模式。即使受害者工作负载的异常延迟触发了事件，一致的延迟模式也可能表明工作负载正在其预期范围内执行，但 I/O 峰值增加了延迟并触发了事件。



如果您最近在访问这些卷工作负载的客户端上安装了一个应用程序，并且该应用程序向它们发送了大量的 I/O，则您可能会预期它们的延迟会增加。如果工作负载的延迟返回到预期范围内，事件状态更改为已过时，并保持此状态超过 30 分钟，则您可能可以忽略该事件。如果事件正在进行中，并且仍处于新状态，则可以进一步进行调查，以确定是否有其他问题导致该事件。

5. 在工作负载吞吐量图表中，选择*恶霸工作负载*以显示恶霸工作负载。

   欺凌工作负载的存在表明，该事件可能是由本地集群上的一个或多个工作负载过度使用 MetroCluster 资源引起的。欺凌工作负载的写入吞吐量（MB/s）偏差较高。

   此图表在较高层级上显示了工作负载的写入吞吐量（MB/s）模式。您可以查看写入 MB/s 模式以识别异常吞吐量，这可能表明工作负载过度使用 MetroCluster 资源。

   如果事件中不涉及恶霸工作负载，则该事件可能是由于集群之间的链路存在运行状况问题或配对集群上的性能问题而引起的。您可以使用 Unified Manager 检查 MetroCluster 配置中两个集群的运行状况。您还可以使用 Unified Manager 检查和分析配对集群上的性能事件。

在 **Active IQ Unified Manager** 中的远程集群上分析 **MetroCluster** 性能事件

您可以使用 Unified Manager 分析 MetroCluster 配置中远程集群上的动态性能事件。该分析可帮助您确定远程集群上的事件是否导致了其伙伴集群上的事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 您必须已在 MetroCluster 配置中分析本地集群上的性能事件，并获得了事件检测时间。
- 您必须已检查参与性能事件的本地集群及其伙伴集群的运行状况，并获取了伙伴集群的名称。

步骤

1. 登录到正在监视配对集群的 Unified Manager 实例。
2. 在左侧导航窗格中，单击*事件*以显示事件列表。
3. 从*时间范围*选择器中，选择*最近一小时*，然后单击*应用范围*。
4. 在*过滤*选择器中，从左侧下拉菜单中选择*集群*，在文本字段中键入伙伴集群的名称，然后单击*应用过滤器*。

   如果在过去一小时内选定集群没有发生任何事件，则表明该集群在其配对节点上检测到事件期间没有遇到任

何性能问题。

5. 如果所选集群在过去一小时内检测到事件，请将事件检测时间与本地集群上事件的事件检测时间进行比较。

   如果这些事件涉及在数据处理组件上引发争用的恶霸工作负载，则其中一个或多个恶霸可能在本地集群上引发该事件。您可以单击事件以对其进行分析，并在事件详细信息页面上查看解决该事件的建议操作。

   如果这些事件不涉及霸道工作负载，则它们并未导致本地集群上发生性能事件。

响应 **Active IQ Unified Manager** 中的动态 **QoS** 限速事件

您可以使用 Unified Manager 调查由服务质量 (QoS) 策略组限制工作负载吞吐量 (MB/s) 引起的性能事件。限制增加了策略组中卷工作负载的响应时间（延迟）。您可以使用事件信息确定是否需要对策略组设置新的限制来停止限制。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须存在新的、已确认的或已过时的性能事件。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 阅读*描述*，其中显示受限流影响的工作负载的名称。

   描述可以为受害者和欺凌者显示相同的工作负载，因为限制会使工作负载本身成为受害者。

3. 使用文本编辑器等应用程序记录卷的名称。

   您可以搜索该卷名称，以便稍后查找。

4. 在 Workload Latency 和 Workload Utilization 图表中，选择 **Bully Workloads**。
5. 将光标悬停在图表上可查看影响策略组的顶级用户定义工作负载。

   列表顶部的工作负载偏差最大，导致限制发生。活动是每个工作负载使用的策略组限制的百分比。

6. 在*建议操作*区域中，单击顶部工作负载的*分析工作负载*按钮。
7. 在“工作负载分析”页面中，将“延迟”图表设置为查看所有集群组件，并将“吞吐量”图表设置为查看明细。

   细分图表显示在延迟图表和 IOPS 图表下方。

8. 比较 延迟 图表中的 QoS 限制，了解事件发生时影响延迟的限制量。

   QoS 策略组的最大吞吐量为每秒 1,000 个操作（op/sec），其中的工作负载总计不能超过此限制。在事件发生时，策略组中的工作负载总吞吐量超过 1,200 op/sec，这导致策略组将其活动限制为 1,000 op/sec。

9. 将*读取/写入延迟*值与*读取/写入/其他*值进行比较。

   两个图表都显示了大量具有高延迟的读取请求，但写入请求的请求数和延迟量较低。这些值可帮助您确定是否存在增加延迟的高吞吐量或操作数。在决定对吞吐量或操作设置策略组限制时，可以使用这些值。

10. 使用 ONTAP System Manager 将策略组的当前限制增加到 1,300 个操作/秒。
11. 一天后，返回 Unified Manager 并在*工作负载分析*页面中输入您在步骤 3 中记录的工作负载。
12. 选择吞吐量分解图。

    此时将显示读取/写入/其他图表。

13. 在页面顶端，将光标指向策略组限制更改的更改事件图标（）。
14. 将*读取/写入/其他*图表与*延迟*图表进行比较。

    读取和写入请求相同，但限制已停止，并且延迟已减少。

响应 **Active IQ Unified Manager** 中由磁盘故障引起的性能事件

您可以使用 Unified Manager 调查由过度使用聚合的工作负载引起的性能事件。您还可以使用 Unified Manager 检查聚合的运行状况，以查看在聚合中检测到的最近运行状况事件是否导致了性能事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须存在新的、已确认的或已过时的性能事件。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 阅读*描述*，其中描述了事件中涉及的工作负载和争用中的集群组件。

    存在多个受集群组件争用影响而导致延迟的受害卷。该聚合正在进行 RAID 重建，以使用备用磁盘替换故障磁盘，是争用中的集群组件。在"争用中的组件"下，聚合图标以红色突出显示，聚合名称显示在括号中。

3. 在 Workload Utilization 图表中，选择 **Bully Workloads**。
4. 将光标悬停在图表上可查看影响组件的排名靠前的霸道工作负载。

    自检测到事件以来，峰值利用率最高的顶级工作负载将显示在图表的顶部。顶级工作负载之一是系统定义的工作负载 Disk Health，它指示 RAID 重建。重建是使用备用磁盘重建聚合的内部过程。Disk Health 工作负载以及聚合上的其他工作负载，可能导致了聚合上的争用及相关事件。

5. 在确认来自磁盘运行状况工作负载的活动导致事件后，等待大约 30 分钟以完成重建，并等待 Unified Manager 分析事件并检测聚合是否仍处于争用状态。
6. 刷新*事件详细信息*。

    RAID 重建完成后，检查状态是否已过时，表示该事件已解决。

7. 在 Workload Utilization 图表中，选择 **Bully Workloads** 以按峰值利用率查看聚合上的工作负载。
8. 在*建议操作*区域中，单击顶部工作负载的*分析工作负载*按钮。
9. 在*工作负载分析*页面中，设置时间范围以显示选定卷的最近 24 小时（1 天）数据。

    在事件时间轴中，红点（）表示磁盘故障事件发生的时间。

10. 在“节点和聚合利用率”图表中，隐藏节点统计信息的线，以便仅保留“聚合”线。
11. 将此图表中的数据与*延迟*图表中事件发生时的数据进行比较。

    在事件发生时，聚合利用率显示由 RAID 重构过程引起的大量读写活动，这增加了所选卷的延迟。事件发生几个小时后，读取和写入以及延迟都已减少，确认聚合不再处于争用状态。

响应 **Active IQ Unified Manager** 中因 **HA** 接管引起的性能事件

您可以使用 Unified Manager 调查由高可用性（HA）对中的群集节点上的高数据处理引起的性能事件。您还可以使用 Unified Manager 检查节点的运行状况，以查看在节点上检测到的任何最近的运行状况事件是否导致了性能事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 必须存在新的、已确认的或已过时的性能事件。

步骤

1. 显示*事件详细信息*页面以查看有关该事件的信息。
2. 阅读*描述*，其中描述了事件中涉及的工作负载和争用中的集群组件。

    有一个受害者卷的延迟受到了发生争用的集群组件的影响。接管了其伙伴节点所有工作负载的数据处理节点是发生争用的集群组件。在“争用组件”下，Data Processing 图标突出显示为红色，并且事件发生时正在进行数据处理的节点名称显示在括号中。

3. 在*描述*中，单击卷的名称。

    此时将显示卷性能资源管理器页面。在页面的顶端，在事件时间线中，更改事件图标（）指示 Unified Manager 检测到 HA 接管开始的时间。

4. 将光标指向 HA 接管的更改事件图标，有关 HA 接管的详细信息将显示在悬停文本中。

    在延迟图表中，一个事件指示所选卷由于与 HA 接管大致相同时间的高延迟而超过性能阈值。

5. 单击*缩放视图*以在新页面上显示延迟图表。
6. 在视图菜单中，选择*集群组件*以按集群组件查看总延迟。
7. 将鼠标光标指向 HA 接管开始时的更改事件图标，并将 Data Processing 的延迟与总延迟进行比较。

    在 HA 接管时，由于数据处理节点上的工作负载需求增加，数据处理量出现了激增。CPU 利用率的增加推高了延迟并触发了该事件。

8. 修复故障节点后，使用 ONTAP System Manager 执行 HA 交还，将工作负载从配对节点移动到已修复的节点。
9. HA 交还完成后，在 Unified Manager 中进行下一次配置发现（大约 15 分钟）后，在*事件管理*清单页面中查找由 HA 接管触发的事件和工作负载。

    由 HA 接管触发的事件现在处于过时状态，这表明该事件已解决。Data Processing 组件的延迟已经降低，从而降低了总延迟。所选卷现在用于 Data Processing 的节点已解决该事件。

解决性能事件

解决 **Active IQ Unified Manager** 中的性能事件

您可以使用建议的操作尝试自行解决性能事件。始终显示前三个建议，第四个建议下的操作特定于显示的事件类型。

*帮助我执行此操作*链接提供了每个建议操作的其他信息，包括执行特定操作的说明。其中一些操作可能涉及使用 Unified Manager、ONTAP System Manager、OnCommand Workflow Automation、ONTAP CLI 命令或这些工具的组合。

确认延迟在 **Active IQ Unified Manager** 中处于预期范围内

当集群组件处于争用状态时，使用它的卷工作负载的响应时间（延迟）可能会变长。您可以查看争用组件上每个受影响工作负载的延迟，以确认其实际延迟在预期范围内。您还可以单击卷名称以查看该卷的历史数据。

如果性能事件处于过时状态，则事件中涉及的每个受害者的延迟可能已恢复到其预期范围内。

评估配置更改如何影响 **Active IQ Unified Manager** 中的工作负载性能

集群上的配置更改（例如磁盘故障、HA 故障转移或移动的卷）可能会对卷性能产生负面影响并导致延迟增加。

在 Unified Manager 中，您可以查看“工作负载分析”页面，以查看最近的配置更改何时发生，并将其与操作和延迟（响应时间）进行比较，以查看选定卷工作负载的活动是否发生变化。

Unified Manager 的性能页面只能检测有限数量的更改事件。运行状况页面为配置更改引起的其他事件提供警报。您可以在 Unified Manager 中搜索卷以查看事件历史记录。

通过在 **Active IQ Unified Manager** 中调整客户端设置来提高工作负载性能

您可以检查向性能事件中涉及的卷发送 I/O 的客户端工作负载（如应用程序或数据库），以确定客户端更改是否可能解决该事件。

当连接到集群上的卷的客户端增加其 I/O 请求时，集群必须增加工作负载以满足需求。如果您知道哪些客户端对集群上的特定卷有大量 I/O 请求，则可以通过调整访问卷的客户端数量或减少对卷的 I/O 量来提高集群性能。您还可以对卷所属的 QoS 策略组应用或增加限制。

您可以调查客户端及其应用程序，以确定客户端发送的 I/O 是否比平时多，这可能会导致群集组件发生争用。在“事件详细信息”页面上，“系统诊断”部分显示使用争用组件的最高卷工作负载。如果您知道哪个客户端正在访问特定卷，则可以转到客户端以确定客户端硬件或应用程序是否未按预期运行或正在执行比平常更多的工作。

在 MetroCluster 配置中，对本地集群上卷的写入请求会被镜像到远程集群上的卷。使本地集群上的源卷与远程集群上的目标卷保持同步，也会增加 MetroCluster 配置中两个集群的需求。通过减少对这些镜像卷的写入请求，集群可以执行更少的同步操作，从而降低对其他工作负载的性能影响。

了解客户端或网络问题如何影响 **Active IQ Unified Manager** 中的性能

当连接到集群上的卷的客户端增加其 I/O 请求时，集群必须更加努力地满足需求。对集群需求的增加可能会使组件处于竞争状态，增加使用它的工作负载的延迟，并触发 Unified Manager 中的事件。

在“事件详细信息”页面上，“系统诊断”部分显示使用争用组件的最高卷工作负载。如果您知道哪个客户端正在访问特定卷，则可以转到客户端以确定客户端硬件或应用程序是否未按预期运行或正在执行比平常更多的工作。您可能需要联系您的客户端管理员或应用程序供应商寻求帮助。

您可以检查网络基础架构，以确定是否存在硬件问题、瓶颈或竞争性工作负载，这可能会导致集群与连接的客户端之间的 I/O 请求执行速度低于预期。您可能需要联系网络管理员以获取帮助。

分析 **Active IQ Unified Manager** 中 **QoS** 策略组内的高活动量卷

您可以查看活动变化最大的服务质量（QoS）策略组中的工作负载，以确定是否有多个工作负载导致了该事件。您还可以查看其他工作负载是否仍然超出设置的吞吐量限制，或者它们是否已回到其预期的活动范围内。

在事件详细信息页面的系统诊断部分，您可以按活动的峰值偏差对工作负载进行排序，以便在表格顶端显示活动变化最大的工作负载。这些工作负载可能是活动超过设置限制并可能导致事件的“`bullies`”。

您可以导航到每个卷工作负载的工作负载分析页面，以查看其 IOPS 活动。如果工作负载具有非常高的操作活动周期，则可能是导致该事件的原因。您可以更改工作负载的策略组设置，也可以将工作负载移至另一个策略组。

可以使用 ONTAP System Manager 或 ONTAP CLI 命令来管理策略组，如下所示：

- 创建策略组。
- 在策略组中添加或删除工作负载。
- 在策略组之间移动工作负载。
- 更改策略组的吞吐量限制。

移动 **LIF** 以提高 **Active IQ Unified Manager** 中的性能

将逻辑接口（LIF）移动到不太繁忙的端口可以帮助改进负载均衡，协助维护操作和性能调优，并减少间接访问。

间接访问会降低系统效率。当卷工作负载使用不同的节点进行网络处理和数据处理时，就会发生这种情况。为了减少间接访问，您可以重新排列 LIF，这涉及移动 LIF 以使用相同的节点进行网络处理和数据处理。您可以配置负载平衡，使 ONTAP 自动将繁忙的 LIF 移动到不同的端口，或者您也可以手动移动 LIF。

优势	注意事项
• 改善负载均衡。 • 减少间接访问。	移动连接到 CIFS 共享的 LIF 时，访问 CIFS 共享的客户端将断开连接。对 CIFS 共享的任何读取或写入请求都会中断。

使用 ONTAP 命令配置负载平衡。有关详细信息，请参见 ONTAP 网络文档。

您可以使用 ONTAP System Manager 和 ONTAP CLI 命令手动移动 LIF。

在非繁忙时间运行存储效率操作

在 **Active IQ Unified Manager** 中安排在较空闲时段执行存储效率操作

您可以修改处理存储效率操作的策略或计划，以在受影响的卷工作负载不太繁忙时运行。

存储效率操作可能会使用大量的集群 CPU 资源，并成为运行这些操作的卷的欺凌者。如果受害者卷在运行存储效率操作的同时具有高活动性，则其延迟可能会增加并触发事件。

在事件详细信息页面上，系统诊断部分按活动的峰值偏差显示 QoS 策略组中的工作负载，以标识欺凌工作负载。如果您在表格顶部附近看到“`storage efficiency`”，则表明这些操作正在欺凌受害者工作负载。通过修改效率策略或计划以在这些工作负载不太繁忙时运行，可以防止存储效率操作在集群上引起争用。

您可以使用 ONTAP System Manager 管理效率策略。您可以使用 ONTAP 命令管理效率策略和计划。

了解 **Active IQ Unified Manager** 中的存储效率

存储效率使您能够以最低的成本存储最大数量的数据，并在消耗更少空间的同时适应快速的数据增长。NetApp 存储效率策略基于其核心 ONTAP 操作系统和 Write Anywhere File Layout（WAFL）文件系统提供的存储虚拟化和统一存储的内置基础。

存储效率包括使用精简配置、Snapshot 副本、重复数据删除、数据压缩、FlexClone、使用 SnapVault 和卷 SnapMirror 的精简复制、RAID-DP、Flash Cache、Flash Pool 聚合以及支持 FabricPool 的聚合等技术，这些技术有助于提高存储利用率并降低存储成本。

统一存储架构允许您在单个平台上高效地整合存储区域网络（SAN）、网络连接存储（NAS）和辅助存储。

高密度磁盘驱动器，例如配置在 Flash Pool 聚合中或结合 Flash Cache 和 RAID-DP 技术使用的串行高级技术附件（SATA）驱动器，可在不影响性能和弹性的情况下提高效率。

启用 FabricPool 的聚合包括作为本地性能层的全 SSD 聚合或 HDD 聚合（从 ONTAP 9.8 开始）以及您指定为云层的对象存储。配置 FabricPool 可帮助您根据数据是否被频繁访问来管理数据应存储在哪个存储层（本地层或云层）。

精简配置、快照副本、重复数据删除、数据压缩、使用 SnapVault 和卷 SnapMirror 的精简复制以及 FlexClone 等技术可提供更好的节省效果。您可以单独或结合使用这些技术，以实现最大的存储效率。

了解添加磁盘如何影响 **Active IQ Unified Manager** 中的数据重新分配

您可以向聚合添加磁盘，以增加该聚合的存储容量和性能。添加磁盘后，只有在跨添加的磁盘重新分配数据后，才会看到读取性能的提高。

当 Unified Manager 收到由动态阈值或系统定义的性能阈值触发的聚合事件时，您可以使用这些说明：

- 收到动态阈值事件后，在“事件详细信息”页面上，表示争用聚合的集群组件图标将突出显示为红色。

  图标下方（括号内）是聚合的名称，用于标识可以向其添加磁盘的聚合。

- 当您收到系统定义的阈值事件时，在事件详细信息页面上，事件描述文本将列出出现问题的聚合的名称。

  您可以添加磁盘并在此聚合上重新分配数据。

添加到聚合的磁盘必须已存在于集群中。如果集群没有可用的额外磁盘，您可能需要联系您的管理员或购买更多磁盘。您可以使用 ONTAP System Manager 或 ONTAP 命令向聚合添加磁盘。

仅在使用 HDD 和 Flash Pool 聚合时，应重新分配数据。请勿在 SSD 或 FabricPool 聚合上重新分配数据。

通过在 **Active IQ Unified Manager** 中的节点上启用 **Flash Cache** 来提高工作负载性能

您可以通过在集群中的每个节点上启用 Flash Cache™ 智能数据缓存来提高工作负载性能。

Flash Cache 模块或基于 PCIe 的性能加速模块内存模块通过充当智能外部读缓存来优化随机读密集型工作负载的性能。此硬件与 ONTAP 的 WAFL External Cache 软件组件协同工作。

在 Unified Manager 的“事件详细信息”页面上，表示争用中的聚合的集群组件图标会突出显示为红色。在图标下方，括号中是聚合的名称，用于标识该聚合。您可以在聚合所在的节点上启用 Flash Cache。

您可以使用 ONTAP System Manager 或 ONTAP 命令查看是否已安装或启用了 Flash Cache，如果尚未启用，则可以将其启用。以下命令指示是否在特定节点上启用了 Flash Cache： **`cluster::> run local options flexscale.enable`**

有关 Flash Cache 及其使用要求的详细信息，请参见以下技术报告：

"技术报告 3832：Flash Cache 最佳实践指南"

通过在 **Active IQ Unified Manager** 上的存储聚合中启用 **Flash Pool** 来提升工作负载性能

可以通过在聚合上启用 Flash Pool 功能来提高工作负载性能。Flash Pool 是同时包含 HDD 和 SSD 的聚合。HDD 用于主存储，SSD 提供高性能读取和写入缓存，以提高聚合性能。

在 Unified Manager 中，事件详细信息页面显示争用中的聚合的名称。您可以使用 ONTAP System Manager 或 ONTAP 命令查看是否为聚合启用了 Flash Pool。如果您已安装 SSD，则可以使用命令行界面启用它。如果您已安装 SSD，则可以在聚合上运行以下命令以查看是否已启用 Flash Pool： **`cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled`**

在此命令中， *`aggr_name`* 是聚合的名称，例如争用中的聚合。

有关 Flash Pool 及其使用要求的详细信息，请参见_群集 Data ONTAP 物理存储管理指南_。

在 **Active IQ Unified Manager** 中检查 **MetroCluster** 配置运行状况

您可以使用 Unified Manager 查看 IP 或 FC MetroCluster 配置中群集的运行状况。运行状况状态和事件可帮助您确定是否存在可能影响工作负载性能的硬件或软件问题。

如果将 Unified Manager 配置为发送电子邮件警报，则可以检查电子邮件中是否存在本地或远程集群上可能导致

性能事件的任何健康问题。在 Unified Manager GUI 中，您可以选择*事件管理*以查看当前事件列表，然后使用筛选器仅显示 MetroCluster 配置事件。

有关详细信息，请参见 "检查 MetroCluster 配置中集群的运行状况"

在 Active IQ Unified Manager 中验证 MetroCluster 配置

通过确保正确设置 MetroCluster 配置，您可以防止在基于 FC 和 IP 的 MetroCluster 配置中镜像工作负载出现性能问题。您还可以通过更改配置或升级软件或硬件组件来提高工作负载性能。

请参阅 "MetroCluster 文档"，了解有关在 MetroCluster 配置中设置集群的说明，包括光纤通道（FC）交换机、电缆和交换机间链路（ISL）。它还可以帮助您配置 MetroCluster 软件，以便本地和远程集群可以进行通信并镜像卷数据。有关您的 MetroCluster over IP 设置的特定信息，请参阅 "安装 MetroCluster IP 配置"。

您可以将您的 MetroCluster 配置与 "MetroCluster 文档"中的要求进行比较，以确定更改或升级 MetroCluster 配置中的组件是否可以提高工作负载性能。此比较可以帮助您回答以下问题：

- 控制器是否适合您的工作负载？
- 是否需要将 ISL 捆绑包升级到更大的带宽以处理更多吞吐量？
- 是否可以调整交换机上的缓冲区到缓冲区信用（BBC）以增加带宽？
- 如果您的工作负载对固态驱动器（SSD）存储具有高写入吞吐量，是否需要升级 FC 到 SAS 网桥以适应吞吐量？

相关信息

- 有关更换或升级 MetroCluster 组件的信息，请参见 "MetroCluster 文档"。
- 有关升级控制器的信息，请参见 "使用切换和切回升级 MetroCluster FC 配置中的控制器"和 "使用切换和切回升级 MetroCluster IP 配置中的控制器"

在 Active IQ Unified Manager 中将工作负载移动到不同的聚合

您可以使用 Unified Manager 来帮助识别比当前工作负载所在的聚合更不繁忙的聚合，然后可以将选定的卷或 LUN 移动到该聚合。将高性能工作负载移动到不太繁忙的聚合或启用了闪存的聚合，可以使工作负载更高效地运行。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 您必须已记录当前存在性能问题的聚合的名称。
- 您必须已记录聚合接收事件的日期和时间。
- Unified Manager 必须已收集并分析了一个月或更长时间的性能数据。

这些步骤可帮助您确定以下资源，以便将高性能工作负载移动到利用率较低的聚合中：

- 同一集群上利用率较低的聚合
- 当前聚合中性能最高的卷

步骤

1. 确定集群中利用率最低的聚合：
   a. 在*事件*详细信息页面中，单击聚合所在的集群的名称。

      集群详细信息显示在性能/集群登录页面中。

   b. 在*摘要*页面上，单击*托管对象*窗格中的*聚合*。

      此时将显示此集群上的聚合列表。

   c. 单击*利用率*列，按利用率最低对聚合进行排序。

      您还可以识别具有最大*空闲容量*的聚合。这将提供一个潜在聚合列表，您可能希望将工作负载移动到这些聚合上。

   d. 写下要将工作负载移动到的聚合的名称。
2. 从接收到该事件的聚合中识别高性能卷：
   a. 单击存在性能问题的聚合。

      聚合详细信息显示在“性能/聚合资源管理器”页面中。

   b. 从*时间范围*选择器中，选择*过去 30 天*，然后单击*应用范围*。

      这使您能够查看比默认 72 小时更长的性能历史记录周期。您希望移动一个持续使用大量资源的卷，而不仅仅是在过去 72 小时内。

   c. 从*查看和比较*控件中，选择*此聚合上的卷*。

      此时将显示此聚合上的 FlexVol 卷和 FlexGroup 组成卷的列表。

   d. 按最高 MB/s 对卷进行排序，然后按最高 IOPS 对卷进行排序，以查看性能最高的卷。
   e. 写下要移动到其他聚合的卷的名称。
3. 将高性能卷移动到您确定的利用率较低的聚合。

   您可以使用 ONTAP System Manager、OnCommand Workflow Automation、ONTAP 命令或这些工具的组合来执行移动操作。

几天后，请检查您是否从此节点或聚合接收到相同类型的事件。

将工作负载移动到 **Active IQ Unified Manager** 中的其他节点

您可以使用 Unified Manager 帮助识别其他节点上的聚合，该聚合的繁忙程度低于当前运行工作负载的节点，然后您可以将所选卷移动到该聚合。将高性能工作负载移动到不太繁忙的节点上的聚合，可以使两个节点上的工作负载更高效地运行。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 您必须已记录当前存在性能问题的节点的名称。

- 必须已记录节点接收性能事件的日期和时间。
- Unified Manager 必须已收集并分析性能数据一个月或更长时间。

此过程可帮助您确定以下资源，以便将高性能工作负载移动到利用率较低的节点：

- 同一集群中空闲性能容量最大的节点
- 新节点上具有最大空闲性能容量的聚合
- 当前节点上性能最高的卷

步骤

1. 确定集群中具有最大可用性能容量的节点：
   a. 在*事件详细信息*页面上，单击节点所在集群的名称。

      集群详细信息显示在性能/集群登录页面中。

   b. 在*摘要*选项卡上，单击*托管对象*窗格中的*节点*。

      此时将显示此集群上的节点列表。

   c. 单击*已用性能容量*列，按已用最少百分比对节点进行排序。

      这提供了可能需要将工作负载移动到的潜在节点的列表。

   d. 写下要将工作负载移动到的节点的名称。
2. 识别新节点上利用率最低的聚合：
   a. 在左侧导航窗格中，单击*存储* > 聚合，然后从视图菜单中选择*性能* > 所有聚合。

      此时将显示“性能：所有聚合”视图。

   b. 单击*过滤*，从左侧下拉菜单中选择*节点*，在文本字段中键入节点的名称，然后单击*应用过滤器*。

      “性能：所有聚合”视图将与此节点上可用的聚合列表一起重新显示。

   c. 单击*已用性能容量*列，按最少使用对聚合进行排序。

      这提供了可能要将工作负载移动到的潜在聚合的列表。

   d. 写下要将工作负载移动到的聚合的名称。
3. 识别来自接收该事件的节点的高性能工作负载：
   a. 返回此事件的*事件详细信息*页面。
   b. 在*受影响的卷*字段中，单击卷数量的链接。

      此时将显示"Performance: All Volumes （性能：所有卷）"视图，其中包含该节点上卷的筛选列表。

   c. 单击*总容量*列，按分配的最大空间对卷进行排序。

      这提供了可能需要移动的潜在卷的列表。

d. 记下要移动的卷的名称，以及它们所在的当前聚合的名称。

4. 将卷移动到您确定在新节点上具有最大可用性能容量的聚合。

   您可以使用 ONTAP System Manager、OnCommand Workflow Automation、ONTAP 命令或这些工具的组合来执行移动操作。

几天后，您可以检查是否从此节点或聚合接收到相同类型的事件。

在 **Active IQ Unified Manager** 中将工作负载移至其他节点上的聚合

您可以使用 Unified Manager 帮助识别其他节点上的聚合，该聚合的繁忙程度低于当前运行工作负载的节点，然后您可以将所选卷移动到该聚合。将高性能工作负载移动到不太繁忙的节点上的聚合，可以使两个节点上的工作负载更高效地运行。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 您必须已记录当前存在性能问题的节点的名称。
- 必须已记录节点接收性能事件的日期和时间。
- Unified Manager 必须已收集并分析了一个月或更长时间的性能数据。

这些步骤可帮助您确定以下资源，以便将高性能工作负载移动到利用率较低的节点：

- 同一集群上利用率较低的节点
- 新节点上利用率最低的聚合
- 当前节点上性能最高的卷

步骤

1. 确定集群中利用率最低的节点：
   a. 在*事件*详细信息页面中，单击节点所在集群的名称。

      集群详细信息显示在性能/集群登录页面中。

   b. 在*摘要*页面上，单击*托管对象*窗格中的*节点*。

      此时将显示此集群上的节点列表。

   c. 单击*利用率*列，按利用率最低对节点进行排序。

      您还可以识别具有最大*可用容量*的节点。这提供了一个潜在节点列表，您可能希望将工作负载移动到这些节点。

   d. 写下要将工作负载移动到的节点的名称。
2. 识别新节点上利用率最低的聚合：
   a. 在左侧导航窗格中，单击*存储* > 聚合，然后从视图菜单中选择*性能* > 所有聚合。

      此时将显示“性能：所有聚合”视图。

b. 单击*过滤*，从左侧下拉菜单中选择*节点*，在文本字段中键入节点的名称，然后单击*应用过滤器*。

“性能：所有聚合”视图将与此节点上可用的聚合列表一起重新显示。

c. 单击*利用率*列，按利用率最低对聚合进行排序。

您还可以识别具有最大*空闲容量*的聚合。这将提供一个潜在聚合列表，您可能希望将工作负载移动到这些聚合上。

d. 写下要将工作负载移动到的聚合的名称。

3. 识别来自接收该事件的节点的高性能工作负载：

a. 返回此事件的*事件*详细信息页面。

b. 在*受影响的卷*字段中，单击卷数量的链接。

此时将显示"Performance: All Volumes （性能：所有卷）"视图，其中包含该节点上卷的筛选列表。

c. 单击*总容量*列，按分配的最大空间对卷进行排序。

这提供了可能需要移动的潜在卷的列表。

d. 记下要移动的卷的名称，以及它们所在的当前聚合的名称。

4. 将卷移动到您确定在新节点上利用率较低的聚合。

您可以使用 ONTAP System Manager、OnCommand Workflow Automation、ONTAP 命令或这些工具的组合来执行移动操作。

几天后，请检查您是否从此节点或聚合接收到相同类型的事件。

将工作负载移动到 **Active IQ Unified Manager** 中不同 **HA** 对的节点

您可以使用 Unified Manager 帮助识别不同高可用性（HA）对中的节点上的聚合，该节点具有比当前运行工作负载的 HA 对更多的可用性能容量。然后，您可以将所选卷移动到新 HA 对上的聚合。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 您的集群必须至少由两个 HA 对组成

如果集群中只有一个 HA 对，则无法使用此修正过程。

- 您必须已记录 HA 对中当前存在性能问题的两个节点的名称。
- 您必须已记录节点接收性能事件的日期和时间。
- Unified Manager 必须已收集并分析性能数据一个月或更长时间。

将高性能工作负载移动到具有更高空闲性能容量的节点上的聚合，可以使两个节点上的工作负载都能更高效地执行。此过程可帮助您识别以下资源，以便您可以将高性能工作负载移动到在其他 HA 对上具有更多空闲性能容量的节点：

- 同一集群上具有最大空闲性能容量的不同 HA 对中的节点
- 具有最大空闲性能容量的新节点上的聚合
- 当前节点上性能最高的卷

步骤

1. 识别属于同一集群上不同 HA 对的节点：
   a. 在*事件详细信息*页面上，单击节点所在的集群的名称。

      集群详细信息显示在性能/集群登录页面中。

   b. 在*摘要*页面上，单击*托管对象*窗格中的*节点*。

      此集群上的节点列表显示在性能：所有节点视图中。

   c. 记下不属于当前存在性能问题的 HA 对的其他 HA 对中的节点名称。
2. 确定新 HA 对中具有最大可用性能容量的节点：
   a. 在*性能：所有节点*视图上，单击*已用性能容量*列，按已用最少百分比对节点进行排序。

      这提供了可能需要将工作负载移动到的潜在节点的列表。

   b. 写下要将工作负载移动到的不同 HA 对上的节点的名称。
3. 确定具有最大空闲性能容量的新节点上的聚合：
   a. 在*性能：所有节点*视图上，单击该节点。

      该节点的详细信息显示在性能/节点资源管理器页面中。

   b. 在*查看和比较*菜单中，选择*此节点上的聚合*。

      此节点上的聚合显示在网格中。

   c. 单击*已用性能容量*列，按最少使用对聚合进行排序。

      这提供了可能要将工作负载移动到的潜在聚合的列表。

   d. 写下要将工作负载移动到的聚合的名称。
4. 从接收事件的节点中识别高性能工作负载：
   a. 返回此事件的*事件*详细信息页面。
   b. 在*受影响的卷*字段中，单击第一个节点的卷数量的链接。

      此时将显示"Performance: All Volumes （性能：所有卷）"视图，其中包含该节点上卷的筛选列表。

   c. 单击*总容量*列，按分配的最大空间对卷进行排序。

      这提供了可能需要移动的潜在卷的列表。

   d. 记下要移动的卷的名称，以及它们所在的当前聚合的名称。

e. 对属于此事件的第二个节点执行步骤 4c 和 4d，以确定可能也要从该节点移动的卷。

5. 将卷移动到您确定在新节点上具有最大可用性能容量的聚合。

   您可以使用 ONTAP System Manager、OnCommand Workflow Automation、ONTAP 命令或这些工具的组合来执行移动操作。

几天后，您可以检查是否从此节点或聚合接收到相同类型的事件。

将工作负载移动到 **Active IQ Unified Manager** 中不同 **HA** 对中的另一个节点

您可以使用 Unified Manager 帮助识别不同 HA 对中节点上的聚合，该节点的繁忙程度低于当前运行工作负载所在的 HA 对。然后，您可以将所选卷移动到新 HA 对上的聚合。将高性能工作负载移动到不太繁忙的节点上的聚合中，可以使两个节点上的工作负载更高效地运行。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 您的集群必须至少由两个 HA 对组成；如果集群中只有一个 HA 对，则不能使用此补救过程。
- 您必须已记录 HA 对中当前存在性能问题的两个节点的名称。
- 您必须已记录节点接收性能事件的日期和时间。
- Unified Manager 必须已收集并分析了一个月或更长时间的性能数据。

这些步骤可帮助您识别以下资源，以便将高性能工作负载移动到其他 HA 对上利用率较低的节点：

- 同一集群中不同 HA 对中利用率较低的节点
- 利用率最低的新节点上的聚合
- 当前节点上性能最高的卷

步骤

1. 识别属于同一集群上不同 HA 对的节点：
   a. 在左侧导航窗格中，单击*存储* > 集群，然后从视图菜单中选择*性能* > 所有集群。

      此时将显示“性能：所有群集”视图。

   b. 单击当前集群的*节点数量*字段中的数字。

      此时将显示“性能：所有节点”视图。

   c. 记录下与当前存在性能问题的 HA 对不同的其他 HA 对中的节点名称。
2. 确定新 HA 对中利用率最低的节点：
   a. 单击*利用率*列，按利用率最低对节点进行排序。

      您还可以识别具有最大*可用容量*的节点。这提供了一个潜在节点列表，您可能希望将工作负载移动到这些节点。

b. 写下要将工作负载移动到的节点的名称。

3. 识别新节点上利用率最低的聚合：

a. 在左侧导航窗格中，单击*存储* > 聚合，然后从视图菜单中选择*性能* > 所有聚合。

此时将显示“性能：所有聚合”视图。

b. 单击*过滤*，从左侧下拉菜单中选择*节点*，在文本字段中键入节点的名称，然后单击*应用过滤器*。

“性能：所有聚合”视图将与此节点上可用的聚合列表一起重新显示。

c. 单击*利用率*列，按利用率最低对聚合进行排序。

您还可以识别具有最大*空闲容量*的聚合。这将提供一个潜在聚合列表，您可能希望将工作负载移动到这些聚合上。

d. 写下要将工作负载移动到的聚合的名称。

4. 从接收事件的节点中识别高性能工作负载：

a. 返回此事件的*事件*详细信息页面。

b. 在*受影响的卷*字段中，单击第一个节点的卷数量的链接。

此时将显示"Performance: All Volumes （性能：所有卷）"视图，其中包含该节点上卷的筛选列表。

c. 单击*总容量*列，按分配的最大空间对卷进行排序。

这提供了可能需要移动的潜在卷的列表。

d. 记下要移动的卷的名称，以及它们所在的当前聚合的名称。

e. 对属于此事件的第二个节点执行步骤 4c 和 4d，以确定可能也要从该节点移动的卷。

5. 将卷移动到您确定在新节点上利用率较低的聚合。

您可以使用 ONTAP System Manager、OnCommand Workflow Automation、ONTAP 命令或这些工具的组合来执行移动操作。

几天后，请检查您是否从此节点或聚合接收到相同类型的事件。

使用 **QoS** 策略设置对 **Active IQ Unified Manager** 中的节点工作负载进行优先级排序

可以对 QoS 策略组设置限制，以控制其包含的工作负载的每秒 I/O （IOPS） 或 MBps 吞吐量限制。如果工作负载位于没有设置限制的策略组中，例如默认策略组，或者设置的限制不满足您的需求，则可以增加设置的限制，或者将工作负载移动到具有所需限制的新策略组或现有策略组。

如果节点上的性能事件是由工作负载过度使用节点资源引起的，则“事件详细信息”页面上的事件描述将显示指向相关卷列表的链接。在“性能/卷”页面中，您可以按 IOPS 和 MBps 对受影响的卷进行排序，以查看哪些工作负载的使用率最高，从而可能导致了该事件。

通过将过度使用节点资源的卷分配给更严格的策略组设置，策略组会限制工作负载以限制其活动，从而可以减少该节点上资源的使用。

可以使用 ONTAP System Manager 或 ONTAP 命令来管理策略组，包括以下任务：

- 创建策略组
- 在策略组中添加或删除工作负载
- 在策略组之间移动工作负载
- 更改策略组的吞吐量限制

删除 **Active IQ Unified Manager** 中的非活动卷和 **LUN**

当聚合可用空间被识别为问题时，您可以搜索未使用的卷和 LUN 并将其从聚合中删除。这有助于缓解磁盘空间不足的问题。

如果聚合中的性能事件是由磁盘空间不足引起的，则有几种方法可以确定哪些卷和 LUN 不再被使用。

识别未使用的卷：

- 在事件详细信息页面上，*受影响的对象计数*字段提供了一个显示受影响卷列表的链接。

  单击此链接在“性能：所有卷”视图上显示卷。在此处，您可以按 **IOPS** 对受影响的卷进行排序，以查看哪些卷未处于活动状态。

要识别未使用的 LUN：

1. 在事件详细信息页面中，记下发生事件的聚合的名称。
2. 在左侧导航窗格中，单击*存储* > **LUN**，然后从视图菜单中选择*性能* > 所有 **LUN**。
3. 单击*过滤*，从左侧下拉菜单中选择*聚合*，在文本字段中键入聚合的名称，然后单击*应用过滤器*。
4. 按 **IOPS** 对受影响 LUN 的结果列表进行排序以查看未处于活动状态的 LUN。

确定未使用的卷和 LUN 后，您可以使用 ONTAP System Manager 或 ONTAP 命令删除这些对象。

了解添加磁盘如何影响 **Active IQ Unified Manager** 中的聚合布局

您可以向聚合添加磁盘，以增加该聚合的存储容量和性能。添加磁盘后，只有在重建聚合后才会看到性能提升。

当您在“事件详细信息”页面上收到系统定义的阈值事件时，事件描述文本会列出出现问题的聚合的名称。您可以在此聚合上添加磁盘和重建数据。

添加到聚合的磁盘必须已存在于集群中。如果集群没有可用的额外磁盘，您可能需要联系您的管理员或购买更多磁盘。您可以使用 ONTAP System Manager 或 ONTAP 命令向聚合添加磁盘。

"技术报告 3838：《存储子系统配置指南》"

在 **Unified Manager** 服务器和外部数据提供程序之间建立连接

在 **Active IQ Unified Manager** 和外部数据提供程序之间建立连接

通过 Unified Manager 服务器和外部数据提供程序之间的连接，您可以将集群性能数据发送到外部服务器，以便存储管理员可以使用第三方软件绘制性能指标图表。

Unified Manager 服务器和外部数据提供程序之间的连接是通过维护控制台中标记为“**外部数据提供程序**”的菜单选项建立的。

将 **Active IQ Unified Manager** 性能数据发送到外部服务器

Unified Manager 从其监控的所有集群收集各种性能数据。您可以将特定数据组发送到外部服务器。

根据要绘制的性能数据，可以选择发送以下统计信息组之一：

统计组	包含的数据	详细信息
性能监视器	以下对象的高级性能统计信息： • LUN 数 • 卷	此组为所有受监视群集中的所有 LUN 和卷提供总 IOPS 或延迟。 此组提供的统计数据数量最少。
资源利用率	以下对象的资源利用率统计信息： • 节点 • 聚合	此组提供所有受监视集群中节点和聚合物理资源的利用率统计信息。 它还提供在性能监视器组中收集的统计信息。
向下钻取	所有跟踪对象的底层读/写和各协议统计信息： • 节点 • 聚合 • LUN 数 • 卷 • 磁盘 • LIF • 端口/NIC	此组提供所有受监控集群中所有七种跟踪对象类型的读/写和每协议细分。 它还提供在性能监视器组和资源利用率组中收集的统计信息。 此组提供最大数量的统计数据。

如果在存储系统上更改了群集或群集对象的名称，则旧对象和新对象都将包含外部服务器上的性能数据（称为“`metric_path`”）。这两个对象不会作为同一个对象相关联。例如，如果将卷的名称从“`volume1_acct`”更改为“`acct_vol1`”，则会看到旧卷的旧性能数据和新卷的新性能数据。

有关可以发送给外部数据提供程序的所有性能计数器的列表，请参阅知识库文章 30096。

"可导出到外部数据提供程序的 Unified Manager 性能计数器"

设置 **Graphite** 以从 **Active IQ Unified Manager** 接收性能数据

Graphite 是一种用于从计算机系统收集和绘制性能数据的开放软件工具。必须正确配置 Graphite 服务器和软件，才能从 Unified Manager 接收统计数据。

NetApp 不对特定版本的 Graphite 或其他第三方工具进行测试或验证。

Graphite 服务器未从 Unified Manager 接收卷的性能数据。

根据安装说明安装 Graphite 后，需要进行以下更改以支持从 Unified Manager 进行统计数据传输：

- 在 `/opt/graphite/conf/carbon.conf`文件中，每分钟可以在 `Graphite` 服务器上创建的最大文件数必须设置为 *`200`*（**MAX_CREATES_PER_MINUTE = 200**`）。

  根据配置中的集群数量和您选择发送的统计对象，可能需要初始创建数千个新文件。以每分钟 200 个文件的速度，可能需要 15 分钟或更长时间才能最初创建所有指标文件。创建所有唯一指标文件后，此参数不再相关。

- 如果在使用 IPv6 地址部署的服务器上运行 Graphite，则 `/opt/graphite/conf/carbon.conf` 文件中的 LINE_RECEIVER_INTERFACE 的值必须从 “0.0.0.0” 更改为 “::” (**`LINE_RECEIVER_INTERFACE = ::`**）

- 在 `/opt/graphite/conf/storage-schemas.conf` 文件中，必须使用 `retentions` 参数将频率设置为 5 分钟，将保留期设置为与您的环境相关的天数。

  保留期可以根据您的环境允许尽可能长，但至少有一个保留设置的频率值必须设置为 5 分钟。在以下示例中，使用 `pattern`参数为 `Unified Manager` 定义了一个部分，值将初始频率设置为 `5` 分钟，将保留期设置为 `100` 天： `**[OPM]**

  ```
  pattern = ^netapp-performance\..

  retentions = 5m:100d
  ```

  如果默认供应商标签从“`netapp-performance`”更改为其他内容，则该更改也必须反映在 `pattern` 参数中。

如果 Unified Manager 服务器尝试发送性能数据时 Graphite 服务器不可用，则不会发送数据，并且收集的数据中将存在间隙。

配置 **Active IQ Unified Manager** 与外部数据提供程序之间的连接

Unified Manager 可以将群集性能数据发送到外部服务器。您可以指定发送的统计数据的类型以及发送数据的时间间隔。

开始之前

- 您必须拥有授权的用户 ID 才能登录到 Unified Manager 服务器的维护控制台。
- 您必须具有下列有关外部数据提供程序的信息：
  - 服务器名称或 IP 地址（IPv4 或 IPv6）
  - 服务器默认端口（如果不使用默认端口 2003）

- 必须已配置远程服务器和第三方软件，以便它可以从 Unified Manager 服务器接收统计数据。
- 您必须知道您要发送哪一组统计信息：
  - PERFORMANCE_INDICATOR: 性能监控统计信息
  - RESOURCE_UTILIZATION：资源利用率和性能监视器统计信息
  - DRILL_DOWN：所有统计信息
- 您必须知道要传输统计信息的时间间隔：5、10 或 15 分钟

  默认情况下，Unified Manager 会以 5 分钟为间隔收集统计信息。如果将传输间隔设置为 10（或 15）分钟，则每次传输期间发送的数据量将比使用默认 5 分钟间隔时大两倍（或三倍）。

  如果将 Unified Manager 性能收集时间间隔更改为 10 或 15 分钟，则必须将传输时间间隔更改为等于或大于 Unified Manager 收集时间间隔。

您可以配置一个 Unified Manager 服务器和一个外部数据提供程序服务器之间的连接。

步骤

1. 请以维护用户身份登录到 Unified Manager 服务器的维护控制台。

   此时将显示 Unified Manager 维护控制台提示。

2. 在维护控制台中，键入*外部数据提供程序*菜单选项的编号。

   此时将显示外部服务器连接菜单。

3. 键入*添加/修改服务器连接*菜单选项的编号。

   此时将显示当前服务器连接信息。

4. 出现提示时，键入 `**y**`以继续。
5. 出现提示时，输入目标服务器的 IP 地址或名称以及服务器端口信息（如果与默认端口 2003 不同）。
6. 出现提示时，键入 `**y**`以确认您输入的信息正确无误。
7. 按任意键返回“外部服务器连接”菜单。
8. 键入*修改服务器配置*菜单选项的编号。

   此时将显示当前服务器配置信息。

9. 出现提示时，键入 `**y**`以继续。
10. 出现提示时，请输入要发送的统计信息类型、发送统计信息的时间间隔以及是否要立即启用统计信息的传输：

对于.....	输入.....
统计组 ID	**0** - PERFORMANCE_INDICATOR（默认） **1** - RESOURCE_UTILIZATION **2** - DRILL_DOWN
供应商标记	将在外部服务器上存储统计信息的文件夹的描述性名称。“netapp-performance”是默认名称，但您可以输入其他值。 通过使用点号表示法，您可以定义分层文件夹结构。例如，通过输入 **stats.performance.netapp**，统计信息将位于 **stats** > **performance** > **netapp** 中。
传输间隔	**5** （默认）、 **10** 或 **15** 分钟
启用/禁用	**0** - 禁用 **1** - 启用（默认）

11. 出现提示时，键入 `**y**`以确认您输入的信息正确无误。
12. 按任意键返回“外部服务器连接”菜单。
13. 键入 `**x**`以退出维护控制台。

配置连接后，所选性能数据将按指定的时间间隔发送到目标服务器。需要几分钟时间，指标才会显示在外部工具中。您可能需要刷新浏览器才能查看指标层次结构中的新指标。

监控和管理集群运行状况

Active IQ Unified Manager 状况监控简介

了解 Active IQ Unified Manager 运行状况监控

Active IQ Unified Manager（以前称为 OnCommand Unified Manager）可帮助您通过集中式用户界面监控大量运行 ONTAP 软件的系统。Unified Manager 服务器基础架构提供可扩展性、可支持性以及增强的监控和通知功能。

Unified Manager 的主要功能包括监控、警报、管理集群的可用性和容量、管理保护功能以及将诊断数据捆绑并发送给技术支持。

您可以使用 Unified Manager 监控您的群集。当群集中出现问题时，Unified Manager 会通过事件通知您有关此类问题的详细信息。某些事件还为您提供了补救措施，您可以采取这些措施来纠正问题。您可以配置事件警报，以便在出现问题时通过电子邮件和 SNMP 陷阱通知您。

您可以使用 Unified Manager 将环境中的存储对象与标注关联起来以管理这些存储对象。您可以创建自定义标注，并通过规则将集群、存储虚拟机（SVM）和卷与标注动态关联起来。

您还可以使用容量和运行状况图表中提供的相应集群对象的信息来规划集群对象的存储要求。

物理和逻辑容量

Unified Manager 使用用于 ONTAP 存储对象的物理和逻辑空间的概念。

- 物理容量：物理空间是指卷中使用的物理存储块。由于存储效率功能（如重复数据删除和压缩）减少了数据，“物理已用容量”通常小于逻辑已用容量。
- 逻辑容量：逻辑空间是指卷中的可用空间（逻辑块）。逻辑空间是指如何使用理论空间，而不考虑重复数据删除或压缩的结果。“已用逻辑空间”是指已用物理空间加上已配置的存储效率功能（例如重复数据删除和压缩）所节省的空间。此测量值通常看起来大于已用物理容量，因为它未反映数据压缩和其他物理空间缩减。因此，总逻辑容量可能高于调配的空间。

容量测量单位

Unified Manager 基于 1024（2^{10}）字节的二进制单位计算存储容量。在 ONTAP 9.10.0 及更早版本中，这些单位显示为 KB、MB、GB、TB 和 PB。从 ONTAP 9.10.1 开始，它们在 Unified Manager 中显示为 KiB、MiB、GiB、TiB 和 PiB。

对于所有版本的 ONTAP，吞吐量使用的单位仍然是千字节/秒（Kbps）、兆字节/秒（Mbps）、千兆字节/秒（Gbps）或太字节/秒（Tbps）等等。

ONTAP 9.10.0 及更早版本的 **Unified Manager** 中显示的容量单位	**ONTAP 9.10.1** 的 **Unified Manager** 中显示的容量单位	计算方式	值（字节）
KB	KiB	1024	1024 字节
MB	MiB	1024 * 1024	1,048,576 字节

ONTAP 9.10.0 及更早版本的 **Unified Manager** 中显示的容量单位	**ONTAP 9.10.1** 的 **Unified Manager** 中显示的容量单位	计算方式	值（字节）
GB	GiB	1024 * 1024 * 1024	1,073,741,824 字节
TB	TiB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 字节

了解**Active IQ Unified Manager**运行状况监控功能

Unified Manager 构建在服务器基础架构之上，可提供可扩展性、可支持性以及增强的监控和通知功能。Unified Manager 支持监控运行 ONTAP 软件的系统。

Unified Manager 包括以下功能：

- 安装了 ONTAP 软件的系统的发现、监控和通知：
  - 物理对象：节点、磁盘、磁盘架、SFO 对、端口和 Flash Cache
  - 逻辑对象：集群、存储虚拟机（SVM）、聚合、卷、LUN、命名空间、qtree、LIF、Snapshot 副本、接合路径、NFS 共享、SMB 共享、用户和组配额、QoS 策略组和启动器组
  - 协议：CIFS、NFS、FC、iSCSI、NVMe 和 FCoE
  - 存储效率：SSD 聚合、Flash Pool 聚合、FabricPool 聚合、重复数据删除和压缩
  - 保护：SnapMirror 关系（同步和异步）以及 SnapVault 关系
- 查看集群发现和监控状态
- MetroCluster over FC 和 IP 配置：查看和监控集群组件的配置、问题和连接状态。用于 MetroCluster over FC 配置的 MetroCluster 交换机和网桥
- 增强的警报、事件和阈值基础架构
- LDAP、LDAPS、SAML 身份验证和本地用户支持
- RBAC（用于预定义的角色集）
- AutoSupport 和支持包
- 增强的仪表板可显示环境的容量、可用性、保护和性能健康状况
- 卷移动互操作性、卷移动历史记录和连接路径更改历史记录
- 影响范围区域，以图形方式显示受某些故障磁盘、MetroCluster 聚合镜像降级和 MetroCluster 备用磁盘遗留事件等事件影响的资源
- 显示 MetroCluster 事件效果的可能效果区域
- Suggested Corrective Actions（建议纠正措施）区域，显示可以执行的操作，以解决一些故障磁盘、MetroCluster 聚合镜像降级和 MetroCluster 备用磁盘遗留事件等事件
- 可能受影响的资源区域，显示可能受卷离线事件、卷受限事件和精简配置卷空间存在风险事件等事件影响的资源
- 支持带有 FlexVol 或 FlexGroup 卷的 SVM
- 支持监控节点根卷

- 增强 Snapshot 副本监控，包括计算可回收空间和删除 Snapshot 副本
- 存储对象的注释
- 存储对象信息（例如物理和逻辑容量、利用率、空间节约、性能和相关事件）的报告创建和管理
- 与 OnCommand Workflow Automation 集成以执行工作流

  "WFA 下载"

使用 **Active IQ Unified Manager** 界面管理存储系统运行状况

这些部分包含有关 Active IQ Unified Manager 为解决数据存储容量、可用性和保护问题而提供的两个用户界面的信息。这两个 UI 是 Unified Manager Web UI 和维护控制台。

如果要在 Unified Manager 中使用保护功能，还必须安装和配置 OnCommand Workflow Automation (WFA)。

Unified Manager Web UI

Unified Manager Web UI 使管理员能够监控与数据存储容量、可用性和保护相关的集群问题并对其进行故障排除。

这些部分介绍了管理员可以遵循的一些常见工作流程，以便对 Unified Manager Web UI 中显示的存储容量、数据可用性或保护问题进行故障排除。

维护控制台

Unified Manager 维护控制台使管理员能够监视、诊断和解决与 Unified Manager 服务器本身相关的操作系统问题、版本升级问题、用户访问问题和网络问题。如果 Unified Manager Web UI 不可用，则维护控制台是访问 Unified Manager 的唯一方式。

您可以使用此信息访问维护控制台并使用它来解决与 Unified Manager 服务器功能相关的问题。

管理和监控集群及集群对象运行状况

了解集群监控

了解 **Active IQ Unified Manager** 中的集群监控

您可以将群集添加到 Unified Manager 数据库，以监视群集的可用性、容量和其他详细信息，例如 CPU 使用情况、接口统计信息、可用磁盘空间、qtree 使用情况和机箱环境。

如果状态异常或超出预定义阈值，则会生成事件。如果配置为执行此操作，则当事件触发警报时， Unified Manager 会向指定的收件人发送通知。

了解 **Active IQ Unified Manager** 中的节点根卷

您可以使用 Unified Manager 监视节点根卷。最佳做法是，节点根卷应具有足够的容量，以防止节点发生故障。

当节点根卷的已用容量超过节点根卷总容量的 80% 时，会生成“节点根卷空间接近满”事件。您可以为事件配置

警报以获取通知。您可以使用 ONTAP System Manager 或 ONTAP CLI 采取适当的操作来防止节点关闭。

如果集群运行 ONTAP 9.14.1 或更高版本，则监控节点根卷的功能不可用。

了解 **Active IQ Unified Manager** 中节点根聚合的事件和阈值

您可以使用 Unified Manager 监视节点根聚合。最佳做法是在根聚合中厚配置根卷，以防止节点停止。

默认情况下，不会为根聚合生成容量和性能事件。此外，Unified Manager 使用的阈值不适用于节点根聚合。只有技术支持代表才能修改设置以生成这些事件。当技术支持代表修改设置时，容量阈值将应用于节点根聚合。

您可以使用 ONTAP System Manager 或 ONTAP 命令行界面采取适当的措施来防止节点停止。

如果集群运行 ONTAP 9.14.1 或更高版本，则监控节点根聚合的功能不可用。

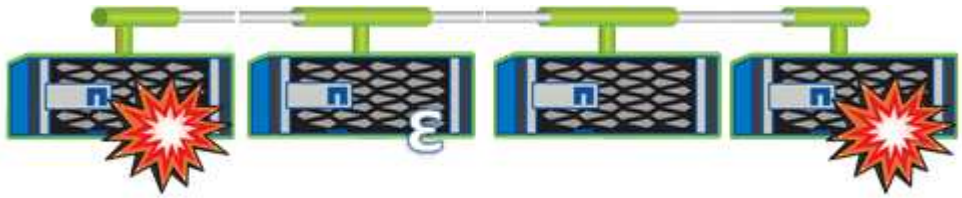
了解 **Active IQ Unified Manager** 集群中的仲裁和 **epsilon**

Quorum 和 epsilon 是衡量集群健康和功能的重要指标，它们共同表明集群如何解决潜在的通信和连接挑战。

仲裁 是集群完全正常运行的前提条件。当集群处于仲裁状态时，大多数节点处于正常运行状态，并且能够相互通信。当仲裁丢失时，集群将失去执行正常集群操作的能力。在任意给定时刻，只有一组节点能够拥有仲裁，因为所有节点共同共享单一的数据视图。因此，如果允许两个无法相互通信的节点以不同的方式修改数据，则将无法再将数据协调为单一的数据视图。

集群中的每个节点都参与一个投票协议，该协议会选举一个节点作为主节点；其余每个节点均为辅助节点。主节点负责在整个集群中同步信息。形成法定人数后，将通过持续投票来维持。如果主节点离线且集群仍处于法定人数状态，则由保持在线的节点选举出新的主节点。

由于具有偶数个节点的集群中可能存在并列，因此一个节点具有称为 epsilon 的额外分数投票权。如果一个大型集群中两个相等部分之间的连接发生故障，而所有节点运行状况均正常，则具有 epsilon 的那组节点将保持仲裁关系。例如，下图显示了一个四节点集群，其中两个节点发生故障。但是，由于其中一个幸存的节点具有 epsilon，因此即使没有大多数运行状况良好的节点，集群仍将保持仲裁状态。



创建集群时，Epsilon 将自动分配给第一个节点。如果持有 epsilon 的节点变得不健康、接管其高可用性配对节点或被其高可用性配对节点接管，则 epsilon 将自动重新分配给不同 HA 对中的健康节点。

使节点离线会影响集群保持仲裁状态的能力。因此，如果您尝试执行会导致集群脱离仲裁，或者使其距离丢失仲裁仅差一次中断的操作， ONTAP 将发出警告消息。您可以在高级权限级别使用 cluster quorum-service options modify 命令来禁用仲裁警告消息。

一般来说，假设集群节点之间具有可靠的连接，较大的集群比较小的集群更稳定。与两个节点的集群相比，在

24 个节点的集群中更容易维持一半节点加 epsilon 的简单多数法定人数要求。

双节点集群在维护仲裁方面存在一些独特的挑战。双节点集群使用集群 HA，其中两个节点均不具有 epsilon；相反，系统会持续轮询这两个节点，以确保如果一个节点发生故障，另一个节点对数据拥有完全读写访问权限，并可访问逻辑接口和管理功能。

在 Active IQ Unified Manager 中查看集群列表和详细信息

您可以使用“运行状况：所有集群”视图来查看集群清单。“容量：所有集群”视图使您可以查看有关所有集群中存储容量和利用率的汇总信息。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

您还可以使用集群/运行状况详细信息页面查看各个集群的详细信息，例如该集群的运行状况、容量、配置、LIF、节点和磁盘。

运行状况：所有群集视图、容量：所有群集视图和群集/运行状况详细信息页面中的详细信息可帮助您规划存储。例如，在配置新的聚合之前，您可以从运行状况：所有群集视图中选择特定群集，并获取容量详细信息以确定群集是否具有所需的空间。

步骤

1. 在左侧导航窗格中，单击 存储 > 集群。
2. 在视图菜单中，选择*运行状况：所有集群*视图以查看运行状况信息，或选择*容量：所有集群*视图以查看所有集群中存储容量和利用率的详细信息。
3. 单击集群名称可在*集群/健康*详细信息页面中查看集群的完整详细信息。

相关信息

- "集群/运行状况详细信息页面"
- "性能：所有集群视图"
- "监控 MetroCluster 配置"
- "查看集群和 Storage VM 的安全状态"
- "正在评估哪些安全标准"

在 Active IQ Unified Manager 中检查 MetroCluster 配置中的集群健康状况

您可以使用 Active IQ Unified Manager （Unified Manager）来检查基于 FC 的 MetroCluster 和基于 IP 的 MetroCluster 配置中集群及其组件的运行状况。如果集群涉及 Unified Manager 检测到的性能事件，则运行状况可以帮助您确定硬件或软件问题是否导致了该事件。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 您必须已分析了 MetroCluster 配置的性能事件，并获得了所涉及集群的名称。

- FC 和 IP 上的 MetroCluster 配置中的两个集群必须由同一个 Unified Manager 实例监控。

确定 FC 配置中 MetroCluster 的集群运行状况

按照以下步骤确定 MetroCluster over FC 配置中的集群运行状况。

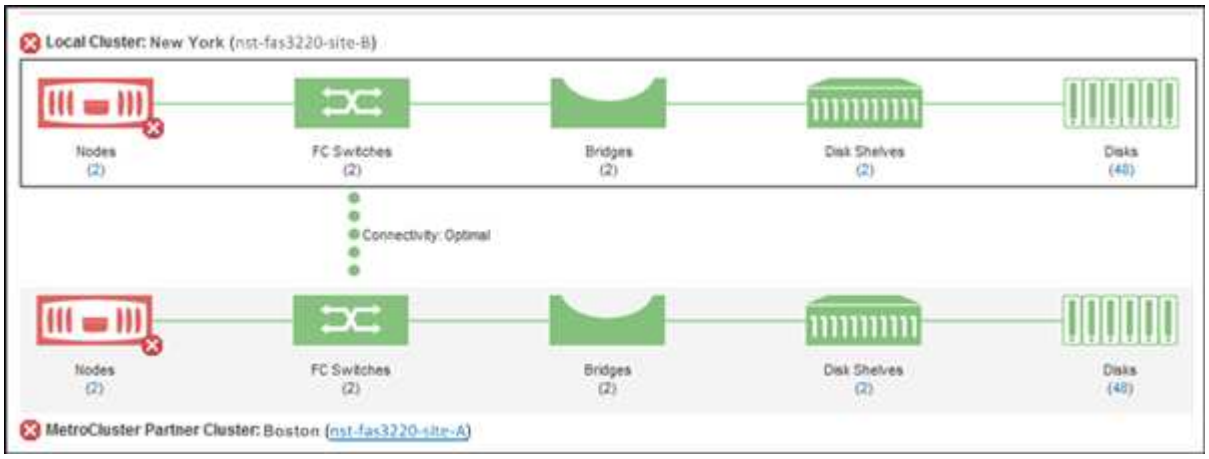
步骤

1. 在左侧导航窗格中，单击*事件管理*以显示事件列表。
2. 在过滤器面板中，选择 源类型 类别下的所有 MetroCluster 过滤器。您可以看到环境中针对所有 MetroCluster 配置引发的所有事件。
3. 在 MetroCluster 事件旁边，单击集群的名称。

   如果没有显示任何 MetroCluster 事件，您可以使用搜索栏搜索与您的 MetroCluster over FC 配置相关的事件中所涉及的集群名称。

   此时将显示“运行状况：所有群集”视图，其中包含有关此事件的详细信息。

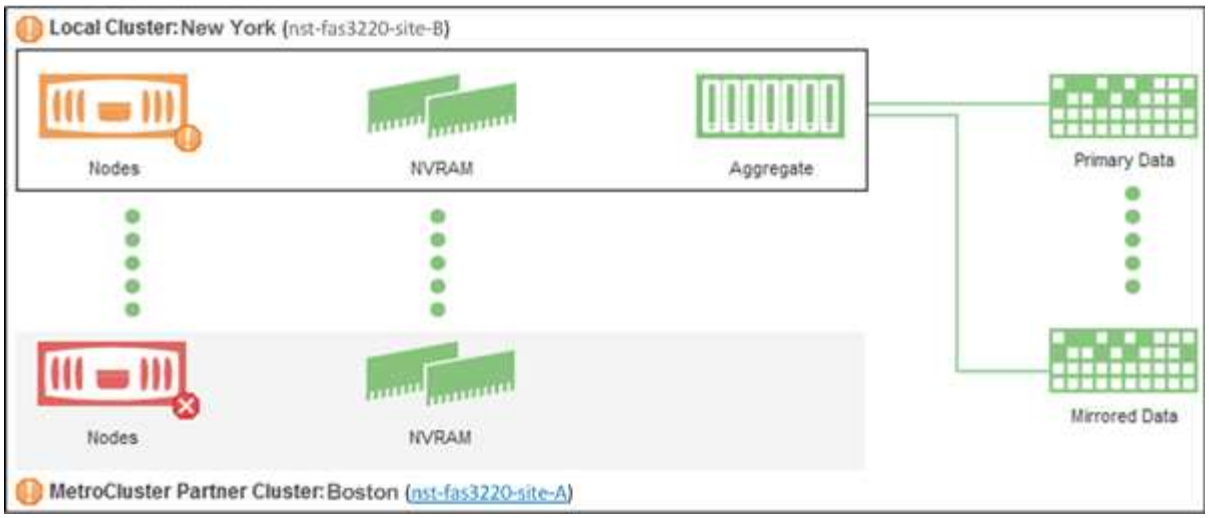
4. 选择 **MetroCluster** 连接 选项卡以显示所选集群与其伙伴集群之间的连接运行状况。



   在此示例中，显示本地群集及其伙伴群集的名称和组件。黄色或红色图标表示突出显示的组件的运行状况事件。“连接”图标表示群集之间的链接。您可以将鼠标光标指向一个图标以显示事件信息，或单击该图标以显示事件。任一群集上的运行状况问题可能导致了性能事件。

   Unified Manager 可监控集群之间链路的 NVRAM 组件。如果本地或合作伙伴集群上的 FC 交换机图标或连接图标为红色，则可能是链路运行状况问题导致了性能事件。

5. 选择 **MetroCluster** 复制 选项卡。



在此示例中，如果本地或合作伙伴群集上的 NVRAM 图标为黄色或红色，则 NVRAM 的运行状况问题可能导致了性能事件。如果页面上没有红色或黄色图标，则可能是合作伙伴群集上的性能问题导致了性能事件。

确定基于 IP 的 MetroCluster 配置中的群集健康状况

请按照以下步骤在 MetroCluster over IP 配置中确定集群健康状况。

步骤

1. 在左侧导航窗格中，单击*事件管理*以显示事件列表。
2. 在筛选器面板的*源类型*类别下，选择 `MetroCluster Relationship`筛选器。您可以看到环境中针对所有 MetroCluster 配置引发的所有事件。

   如果您看不到报告的 MetroCluster 事件，您可以使用搜索栏按与您的基于 IP 的 MetroCluster 配置相关的事件中所涉及的集群名称进行搜索。

3. 在相关 MetroCluster 事件旁边，单击集群的名称。此时将显示包含该集群详细信息的“集群”页面。有关确定运行状况问题的信息，请参阅"监控 MetroCluster over IP 配置中的连接问题"。

在 Active IQ Unified Manager 中查看所有 SAN 阵列集群的运行状况和容量状态

您可以使用群集清单页面显示 All SAN Array 群集的运行状况和容量状态。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

您可以在运行状况：所有集群视图和容量：所有集群视图中查看 All SAN Array 集群的概述信息。此外，您可以在集群/运行状况详细信息页面中查看详细信息。

步骤

1. 在左侧导航窗格中，单击 存储 > 集群。
2. 确保在 运行状况：所有集群 视图中显示 “Personality” 列，或使用 显示 / 隐藏 控件添加它。

   此列为您的 All SAN Array 集群显示 “All SAN Array”。

3. 查看信息。
4. 要查看有关这些群集中存储容量的信息，请选择“容量：所有群集”视图。
5. 要查看有关这些集群中的运行状况和存储容量的详细信息，请单击 All SAN Array 集群的名称。

   在“群集/运行状况详细信息”页面的“运行状况”、“容量”和“节点”选项卡中查看详细信息

在 Active IQ Unified Manager 中查看节点列表和详细信息

您可以使用“运行状况：所有节点”视图查看集群中的节点列表。您可以使用集群/运行状况详细信息页面查看有关受监控集群中节点的详细信息。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

您可以查看详细信息，例如节点状态、包含节点的集群、聚合容量详细信息（已使用和总计）以及原始容量详细信息（可用、备用和总计）。您还可以获取有关 HA 对、磁盘架和端口的信息。

步骤

1. 在左侧导航窗格中，单击*存储* > 节点。
2. 在 健康：所有节点 视图中，单击要查看其详细信息的节点。

   所选节点的详细信息将显示在“群集/运行状况详细信息”页面中。左侧窗格将显示 HA 对列表。默认情况下，HA 详细信息将打开，其中将显示与所选 HA 对相关的 HA 状态详细信息和事件。

3. 要查看节点的其他详细信息，请执行相应的操作：

查看项	单击.....
有关磁盘架的详细信息	磁盘架。
端口相关信息	端口。

有关详细信息，请参见：

- "性能：所有节点视图"
- "查看节点和聚合可用 IOPS 值"
- "查看节点和聚合性能容量使用值"

在 Active IQ Unified Manager 中生成用于合同续签的硬件清单报告

您可以生成一份报告，其中包含完整的集群和节点信息列表；例如硬件型号和序列号、磁盘类型和数量、已安装的许可证等。此报告有助于在未连接到 NetAppActive IQ 平台的安全站点（“暗”站点）内续签合同。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储* > 节点。
2. 转到*健康：所有节点*视图或*性能：所有节点*视图。
3. 选择 报告 > * > 硬件库存报告*。

   硬件库存报告将作为 .csv 文件下载，其中包含截至当前日期的完整信息。

4. 请将这些信息提供给您的 NetApp 支持联系人，以便续订合同。

在 **Active IQ Unified Manager** 中查看 **Storage VM** 列表和详细信息

在运行状况：所有 Storage VM 视图中，您可以监控存储虚拟机 (SVM) 的清单。您可以使用 Storage VM / 运行状况详细信息页面查看有关受监控 SVM 的详细信息。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

您可以查看 SVM 详细信息，例如 SVM 的容量、效率和配置。您还可以查看有关该 SVM 的相关设备和相关警报的信息。

步骤

1. 在左侧导航窗格中，单击 存储 > 存储 **VM**。
2. 选择以下方式之一来查看 SVM 详细信息：
   - 要查看有关所有集群中所有 SVM 运行状况的信息，请在“视图”菜单中选择“运行状况：所有 Storage VM”视图。
   - 要查看完整的详细信息，请单击 Storage VM 名称。

     您还可以通过单击最小详细信息对话框中的*查看详细信息*来查看完整的详细信息。
3. 通过单击最小详细信息对话框中的*查看相关*，查看与 SVM 相关的对象。

相关信息

- "Storage VM：运行状况详细信息页面"
- "性能：所有 Storage VM 视图"
- "安全：反勒索软件视图"
- "查看集群和 Storage VM 的安全状态"
- "关系：所有关系视图"

在 **Active IQ Unified Manager** 中查看聚合列表和详细信息

从“运行状况：所有聚合”视图中，您可以监控聚合清单。“容量：所有聚合”视图使您能够查看有关所有集群中聚合的容量和利用率的信息。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

您可以从聚合/运行状况详细信息页面查看聚合容量和配置以及磁盘信息等详细信息。如果需要，您可以在配置阈值设置之前使用这些详细信息。

步骤

1. 在左侧导航窗格中，单击*存储* > 聚合。
2. 选择以下方式之一来查看聚合详细信息：
   - 要查看有关所有群集中所有聚合的运行状况的信息，请在“查看”菜单中选择“运行状况：所有聚合”视图。
   - 要查看有关所有集群中所有聚合的容量和利用率的信息，请在“视图”菜单中选择“容量：所有聚合”视图。
   - 要查看完整的详细信息，请单击聚合名称。

     您还可以通过单击最小详细信息对话框中的*查看详细信息*来查看完整的详细信息。
3. 通过单击最小详细信息对话框中的*查看相关*，查看与聚合相关的对象。

相关信息

- "聚合/运行状况详细信息页面"
- "性能：所有聚合视图"
- "创建报告以查看 Active IQ Unified Manager 中容量接近上限的聚合"

在 Active IQ Unified Manager 中查看 FabricPool 容量信息

您可以在这些对象的容量和性能清单以及详细信息页面上查看集群、聚合和卷的 FabricPool 容量信息。配置镜像层后，这些页面还会显示 FabricPool 镜像信息。

这些页面显示以下信息：本地性能层和云层上的可用容量、这两个层中正在使用的容量、哪些聚合已附加到云层，以及哪些卷正在通过将某些信息移动到云层来实施 FabricPool 功能。

当云层镜像到另一个云提供商（“镜像层”）时，两个云层都会显示在聚合/运行状况详细信息页面中。

步骤

1. 执行以下操作之一：

要查看……的容量信息	操作
集群	a. 在“容量：所有集群”视图中，单击集群。 b. 在集群/运行状况详细信息页面上，单击 配置 选项卡。 显示屏显示此集群连接到的任何云层的名称。

要查看……的容量信息	操作
聚合	a. 在“容量：所有聚合”视图中，单击“类型”字段指示“SSD (FabricPool)”或“HDD (FabricPool)”的聚合。 b. 在聚合/健康详细信息页面上，单击*容量*选项卡。 此显示屏显示云层中使用的总容量。 c. 单击*磁盘信息*选项卡。 显示屏会显示云层的名称和已用容量。 d. 单击 **Configuration** 选项卡。 此显示屏显示云层的名称以及有关云层的其他详细信息。
卷	a. 在“容量：所有卷”视图上，单击“分层策略”字段中显示策略名称的卷。 b. 在“卷/运行状况详细信息”页面上，单击 配置 选项卡。 显示屏显示分配给该卷的 FabricPool 分层策略的名称。

2. 在*工作负载分析*页面中，您可以在*容量趋势*区域中选择 “云层视图”，以查看上个月本地性能层和云层中使用的容量。

有关 FabricPool 聚合的更多信息，请参见 "磁盘和聚合概述"。

在 **Active IQ Unified Manager** 中查看存储池详细信息

您可以查看存储池的详细信息，以监控存储池的运行状况、总缓存和可用缓存，以及已使用和可用分配。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储* > 聚合。
2. 单击聚合名称。

   将显示所选聚合的详细信息。
3. 单击*磁盘信息*选项卡。

   此时将显示详细的磁盘信息。

仅当所选聚合使用存储池时，才会显示缓存表。

4. 在缓存表中，将指针移到所需存储池的名称上。

   将显示存储池的详细信息。

在 Active IQ Unified Manager 中查看卷列表和详细信息

从“运行状况：所有卷”视图中，您可以监控卷清单。“容量：所有卷”视图使您可以查看有关集群中卷的容量和利用率的信息。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

您还可以使用卷/运行状况详细信息页面查看有关受监控卷的详细信息，包括卷的容量、效率、配置和保护。您还可以查看有关特定卷的相关设备和相关警报的信息。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 从下列方法中选择一种，以查看卷的详细信息：
   - 要查看有关集群中卷运行状况的详细信息，请在“视图”菜单中选择“运行状况：所有卷”视图。
   - 要查看有关集群中卷的容量和利用率的详细信息，请在“视图”菜单中选择“容量：所有卷”视图。
   - 要查看完整的详细信息，请单击卷名。

     您还可以通过单击最小详细信息对话框中的*查看详细信息*来查看完整的详细信息。
3. 可选：*通过单击最小详细信息对话框中的*查看相关，查看与卷相关的对象。

相关信息

- "卷：健康详细信息页面"
- "性能：所有卷视图"
- "安全：反勒索软件视图"
- "查看卷保护关系"
- "创建报告以查看可用卷容量图表"

查看 Active IQ Unified Manager 中 NFS 共享的详细信息

您可以查看有关所有 NFS 共享的详细信息，例如其状态、与卷（FlexGroup 卷或 FlexVol 卷）关联的路径、客户端对 NFS 共享的访问级别以及为导出的卷定义的导出策略。使用运行状况：所有 NFS 共享视图查看所有受监视集群上的所有 NFS 共享，并使用 Storage VM / 运行状况详细信息页面查看特定存储虚拟机（SVM）上的所有 NFS 共享。

开始之前

- 集群上必须启用 NFS 许可证。

- 必须配置为 NFS 共享提供服务的网络接口。
- 您必须具有操作员、应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，根据您是要查看所有 NFS 共享还是仅查看特定 SVM 的 NFS 共享，执行以下步骤。

目的	按照下面的步骤进行操作……
查看所有 NFS 共享	单击 **Storage** > **NFS Shares**
查看单个 SVM 的 NFS 共享	a. 单击 **Storage** > **Storage VMs** b. 单击要查看其 NFS 共享详细信息的 SVM。 c. 在 Storage VM / Health details 页面中，单击 **NFS Shares** 选项卡。

有关详细信息，请参见 "配置文件共享卷" 和 "使用 API 配置 CIFS 和 NFS 文件共享"。

在 Active IQ Unified Manager 中查看有关 SMB/CIFS 共享的详细信息

您可以查看有关所有 SMB/CIFS 共享的详细信息，例如共享名称、接合路径、包含对象、安全设置以及为共享定义的导出策略。使用运行状况：所有 SMB 共享视图查看所有受监视集群上的所有 SMB 共享，并使用 Storage VM / 运行状况详细信息页面查看特定 Storage Virtual Machine （SVM）上的所有 SMB 共享。

开始之前

- 集群上必须已启用 CIFS 许可证。
- 必须配置服务于 SMB/CIFS 共享的网络接口。
- 您必须具有操作员、应用程序管理员或存储管理员角色。

未显示文件夹中的共享。

步骤

1. 在左侧导航窗格中，根据您是要查看所有 SMB/CIFS 共享还是仅查看特定 SVM 的共享，执行以下步骤。

目的	按照下面的步骤进行操作……
查看所有 SMB/CIFS 共享	单击 **Storage** > **SMB Shares**
查看单个 SVM 的 SMB/CIFS 共享	a. 单击 **Storage** > **Storage VMs** b. 单击要查看其 SMB/CIFS 共享详细信息的 SVM。 c. 在 Storage VM / Health 详细信息页面中，单击 **SMB Shares** 选项卡。

有关详细信息，请参见"使用 API 配置 CIFS 和 NFS 文件共享"。

在 **Active IQ Unified Manager** 中查看 **Snapshot** 副本列表

您可以查看选定卷的 Snapshot 副本列表。您可以使用 Snapshot 副本列表来计算在删除一个或多个 Snapshot 副本时可以回收的磁盘空间量，并且可以根据需要删除 Snapshot 副本。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 包含 Snapshot 副本的卷必须处于联机状态。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在 运行状况：所有卷 视图中，选择包含要查看的 Snapshot 副本的卷。
3. 在*卷 / 健康*详细信息页面中，单击*容量*选项卡。
4. 在*容量*选项卡的*详细信息*窗格中，在其他详细信息部分中，单击*快照副本*旁边的链接。

   Snapshot 副本数是一个显示 Snapshot 副本列表的链接。

相关信息

"运行状况/卷页面"

在 **Active IQ Unified Manager** 中删除 **Snapshot** 副本

您可以删除 Snapshot 副本以节省空间或释放磁盘空间，也可以删除不再需要的 Snapshot 副本。

开始之前

您必须具有应用程序管理员或存储管理员角色。

卷必须联机。

要删除忙碌或锁定的 Snapshot 副本，必须从使用该副本的应用程序中释放该 Snapshot 副本。

- 如果 FlexClone 卷正在使用该 Snapshot 副本，则无法删除父卷中的基本 Snapshot 副本。

  基本 Snapshot 副本是用于创建 FlexClone 卷的 Snapshot 副本，并在父卷中显示状态 `Busy`和应用程序依赖关系为 `Busy，Vclone`。

- 无法删除 SnapMirror 关系中使用的锁定 Snapshot 副本。

  Snapshot 副本已锁定，需要在下次更新时使用。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在 运行状况：所有卷 视图中，选择包含要查看的 Snapshot 副本的卷。

此时将显示 Snapshot 副本列表。

3. 在*卷 / 健康*详细信息页面中，单击*容量*选项卡。
4. 在*容量*选项卡的*详细信息*窗格中，在其他详细信息部分中，单击*快照副本*旁边的链接。

   Snapshot 副本数是一个显示 Snapshot 副本列表的链接。

5. 在*Snapshot 副本*视图中，选择要删除的 Snapshot 副本，然后单击*删除选定*。

在 **Active IQ Unified Manager** 中计算 **Snapshot** 副本的可回收空间

如果删除了一个或多个 Snapshot 副本，则可以计算可回收的磁盘空间量。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 卷必须联机。
- 卷必须是 FlexVol 卷；FlexGroup 卷不支持此功能。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在 运行状况：所有卷 视图中，选择包含要查看的 Snapshot 副本的卷。

   此时将显示 Snapshot 副本列表。

3. 在*卷 / 健康*详细信息页面中，单击*容量*选项卡。
4. 在*容量*选项卡的*详细信息*窗格中，在其他详细信息部分中，单击*快照副本*旁边的链接。

   Snapshot 副本数是一个显示 Snapshot 副本列表的链接。

5. 在 **Snapshot** 副本 视图中，选择要计算可回收空间的 Snapshot 副本。
6. 单击*计算*。

   此时将显示卷上的可回收空间（以百分比和 KB、MB、GB 等为单位）。

7. 要重新计算可回收空间，请选择所需的 Snapshot 副本，然后单击 重新计算。

了解 **Active IQ Unified Manager** 中的集群对象窗口和对话框

您可以从相应的存储对象页面查看所有群集和群集对象。您还可以从相应的存储对象详细信息页面查看详细信息。您现在可以从清单的以下存储和保护部分启动 System Manager 用户界面。

- 群集清单、群集运行状况和群集性能页面
- 聚合清单、聚合运行状况和聚合性能页面
- Volume Inventory、Volume Health 和 Volume Performance 页面

- 节点清单和节点性能页面
- StorageVM 清单、StorageVM 运行状况和 StorageVM 性能页面
- 保护关系页面

常见 Unified Manager 运行状况工作流和任务

了解常见 Active IQ Unified Manager 运行状况工作流程和任务

与 Unified Manager 相关的一些常见管理工作流程和任务包括选择要监控的存储集群；诊断对数据可用性、容量和保护产生不利影响的条件；恢复丢失的数据；配置和管理卷；以及捆绑诊断数据并将其发送给技术支持（必要时）。

Unified Manager 使存储管理员能够查看仪表板，评估托管存储集群的整体容量、可用性和保护运行状况，然后快速识别、定位、诊断并分配可能出现的任何特定问题以进行解决。

与群集、存储虚拟机（SVM）、卷或 FlexGroup 卷相关的影响托管存储对象的存储容量或数据可用性的最重要问题将显示在仪表板页面的系统运行状况图和事件中。当发现关键问题时，此页面会提供支持适当故障排除工作流程的链接。

Unified Manager 也可以包含在包含相关可管理性工具（例如 OnCommand Workflow Automation (WFA)）的工作流中，以支持直接配置存储资源。

本文档介绍了与以下管理任务相关的常见工作流程：

- 诊断和管理可用性问题

  如果硬件故障或存储资源配置问题导致在“仪表板”页面中显示数据可用性事件，则存储管理员可以按照嵌入式链接查看有关受影响存储资源的连接信息，查看故障排除建议，并将问题解决方案分配给其他管理员。

- 配置和监控性能事件

  管理员可以监控和管理正在受监控的存储系统资源的性能。有关详细信息，请参见 "Active IQ Unified Manager 性能监控简介"。

- 诊断和管理卷容量问题

  如果在“仪表板”页面中显示卷存储容量问题，存储管理员可以按照嵌入式链接查看与受影响卷的存储容量相关的当前和历史趋势，查看故障排除建议，并将问题解决方案分配给其他管理员。

- 配置、监控和诊断保护关系问题

  在创建和配置保护关系后，存储管理员可以查看与保护关系相关的潜在问题、保护关系的当前状态、有关受影响关系的当前和历史保护作业成功信息以及故障排除建议。有关详细信息，请参见 "了解如何管理和监控保护关系"。

- 创建备份文件并从备份文件还原数据。
- 将存储对象与标注关联

  通过将存储对象与批注相关联，存储管理员可以筛选和查看与存储对象相关的事件，这使存储管理员能够确定优先级并解决与事件相关联的问题。

- 使用 REST API 通过查看 Unified Manager 捕获的运行状况、容量和性能信息来帮助管理集群。有关详细信息，请参见"Active IQ Unified Manager REST API 入门"。
- 向技术支持发送支持包

  存储管理员可以使用维护控制台检索支持包并将其发送给技术支持。当问题需要比 AutoSupport 消息提供的更详细的诊断和故障排除时，必须将支持包发送给技术支持。

监控数据可用性并排除故障

在 **Active IQ Unified Manager** 中监控和排除数据可用性故障

Unified Manager 可监控授权用户访问您存储数据的可靠性，提醒您注意阻止或阻碍该访问的情况，并使您能够诊断这些情况以及分配和跟踪其解决过程。

本节中的可用性工作流程主题介绍了存储管理员如何使用 Unified Manager Web UI 来发现、诊断并分配解决对数据可用性产生不利影响的硬件和软件状况的示例。

扫描并解决存储故障转移互连链路断开情况

扫描并解决 **Active IQ Unified Manager** 中的存储故障转移互连链路中断情况

此工作流程提供了如何扫描、评估和解决已关闭的存储故障转移互连链路条件的示例。在这种情况下，在节点上开始 ONTAP 版本升级之前，您是使用 Unified Manager 扫描存储故障转移风险的管理员。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

如果 HA 对节点之间的存储故障转移互连在无中断升级尝试期间失败，则升级将失败。因此，通常的做法是管理员在开始升级之前监控并确认计划进行升级的集群节点上的存储故障转移可靠性。

步骤

1. 在左侧导航窗格中，单击*事件管理*。
2. 在*事件管理*清单页面中，选择*活动可用性事件*。
3. 在 事件管理 清单页面 名称 列顶端，单击 并在文本框中输入 `*failover`，以将要显示的事件限制为与存储故障转移相关的事件。

   显示与存储故障转移条件相关的所有过去事件。

   在这种情况下，Unified Manager 会在其可用性事件部分显示事件“`Storage Failover Interconnect One or More Links Down`”。

4. 如果一个或多个与存储故障转移相关的事件显示在 事件管理 清单页面上，请执行以下步骤：

   a. 单击事件标题链接以显示该事件的事件详细信息。

      在此示例中，单击事件标题“`Storage Failover Interconnect One or More Links Down`”。此时将显示此事件的“事件详细信息”页面。

a. 在“事件详细信息”页面上，您可以执行以下一个或多个任务：
   - 查看“原因”字段中的错误消息并评估问题。
   - 将此事件分配给管理员。
   - 请确认此事件。

相关信息

"事件详细信息页面"

"Unified Manager 用户角色和功能"

在 **Active IQ Unified Manager** 中对存储故障转移互连链路故障执行更正操作

显示存储故障转移相关事件的“事件详细信息”页面时，可以查看该页面的摘要信息，以确定事件的紧迫性、问题的可能原因以及问题的可能解决方案。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

在此示例场景中，事件详细信息页面上提供的事件摘要包含有关存储故障转移互连链路关闭情况的以下信息：

```
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)
```

示例事件信息指示 HA 对节点 aardvark 和 bonobo 之间的存储故障转移互连链路 Link1 已关闭，但 Apple 和 Boy 之间的 Link0 处于活动状态。由于有一个链路处于活动状态，远程动态内存访问（RDMA）仍在运行，存储故障转移作业仍可成功。

但是，为了防止两条链路均发生故障而导致存储故障转移保护完全禁用，您决定进一步诊断 Link1 中断的原因。

步骤

1. 从*事件*详细信息页面，您可以单击“源”字段中指定事件的链接，以获取可能与存储故障转移互连链路关闭

条件相关的其他事件的更多详细信息。

在此示例中，事件的源是名为 aardvark 的节点。单击该节点名称会在“群集/运行状况详细信息”页面的“节点”选项卡上显示受影响的 HA 对（aardvark 和 bonobo）的 HA 详细信息，并显示最近在受影响的 HA 对上发生的其他事件。

2. 请查看 **HA** 详细信息 以了解有关此事件的更多信息。

   在此示例中，相关信息位于事件表中。该表显示了“`Storage Failover Connection One or More Link Down`”事件、该事件的生成时间以及该事件的源节点。

使用 HA 详细信息中的节点位置信息，请求或亲自完成对受影响 HA 对节点上存储故障转移问题的物理检查和修复。

相关信息

"事件详细信息页面"

"Unified Manager 用户角色和功能"

解决卷脱机问题

解决 **Active IQ Unified Manager** 中的卷脱机问题

此工作流程提供了如何评估和解决 Unified Manager 可能在事件管理清单页面中显示的卷脱机事件的示例。在此场景中，您是使用 Unified Manager 对一个或多个卷脱机事件进行故障排除的管理员。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

卷可能因以下几个原因被报告为离线：

- SVM 管理员已故意使卷脱机。
- 卷的托管集群节点已关闭，并且到其 HA 对伙伴的存储故障转移也已失败。
- 卷的托管存储虚拟机（SVM）已停止，因为托管该 SVM 的根卷的节点已停机。
- 由于两个 RAID 磁盘同时出现故障，此卷的托管聚合已关闭。

您可以使用事件管理清单页面以及群集/运行状况、存储虚拟机/运行状况和卷/运行状况详细信息页面来确认或消除其中一种或多种可能性。

步骤

1. 在左侧导航窗格中，单击*事件管理*。
2. 在*事件管理*清单页面中，选择*活动可用性事件*。
3. 单击为“Volume Offline”事件显示的超文本链接。

   此时将显示可用性意外事件的“事件详细信息”页面。

4. 在该页面上，查看备注，以确定是否有迹象表明 SVM 管理员已将相关卷脱机。

5. 在*事件*详细信息页面上，您可以查看以下一个或多个任务的信息：
   - 查看“原因”字段中显示的信息，以获得可能的诊断指导。

     在此示例中，“原因”字段中的信息仅通知您此卷已脱机。

   - 检查 Notes and Updates（注释和更新）区域，查看是否有任何迹象表明 SVM 管理员故意使相关卷脱机。
   - 单击事件源（在本例中为离线报告的卷）以获取有关该卷的详细信息。
   - 将此事件分配给管理员。
   - 请确认该事件，或在适当情况下将其标记为已解决。

在 **Active IQ Unified Manager** 中对卷脱机情况执行诊断操作

导航到报告为离线的卷的卷/运行状况详细信息页面后，您可以搜索有助于诊断卷离线状况的其他信息。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

如果报告为脱机的卷不是有意脱机的，则该卷可能由于多种原因而处于脱机状态。

从离线卷的“卷/运行状况”详细信息页面开始，您可以导航到其他页面和窗格以确认或排除可能的原因：

- 单击 卷/运行状况 详细信息页面链接，以确定卷是否处于脱机状态，因为其主机节点已停机，并且向其 HA 对配对节点进行的存储故障转移也已失败。

  请参阅 "确定卷离线状态是否由停机节点引起"。

- 单击 卷/运行状况 详细信息页面链接，以确定卷是否处于脱机状态，以及其主机存储虚拟机 (SVM) 是否因托管该 SVM 根卷的节点已停机而停止。

  请参阅 "确定卷是否脱机以及 SVM 是否因节点关闭而停止"。

- 单击 卷 / 运行状况 详细信息页面链接，以确定卷是否由于其主机聚合中的磁盘损坏而处于脱机状态。

  请参阅 "确定卷是否由于聚合中的磁盘损坏而处于脱机状态"。

相关信息

"Unified Manager 用户角色和功能"

确定卷是否因其主机节点在 **Active IQ Unified Manager** 中关闭而处于脱机状态

您可以使用 Unified Manager Web UI 确认或排除卷因其主机节点已关闭且向其 HA 对伙伴的存储故障转移不成功而脱机的可能性。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

要确定卷离线状态是否由托管节点故障和随后不成功的存储故障转移引起，请执行以下操作：

步骤

1. 在离线卷的 **Volume / Health** 详细信息页面的 **Related Devices** 窗格中，找到并单击 SVM 下显示的超文本链接。

   Storage VM / Health 详细信息页面显示有关脱机卷的托管 Storage Virtual Machine (SVM) 的信息。

2. 在 **Storage VM / Health** 详细信息页面的 **Related Devices** 窗格中，找到并单击 Volumes 下显示的超文本链接。

   运行状况：所有卷视图显示有关由 SVM 托管的所有卷的信息表。

3. 在 运行状况：所有卷 视图的“状态”列标题上，单击筛选器符号 ，然后选择 脱机 选项。

   仅列出处于离线状态的 SVM 卷。

4. 在“运行状况：所有卷”视图中，单击网格符号 ，然后选择 集群节点 选项。

   您可能需要在网格选择框中滚动以找到*集群节点*选项。

   集群节点列将添加到卷清单中，并显示托管每个脱机卷的节点的名称。

5. 在 运行状况：所有卷 视图中，找到离线卷的列表，并在其集群节点列中单击其托管节点的名称。

   “集群/健康”详细信息页面上的“节点”选项卡显示托管节点所属的 HA 节点对的状态。托管节点的状态和任何集群故障转移操作的成功情况都会予以显示。

在确认由于其主机节点已关闭并且到 HA 对伙伴的存储故障转移失败而存在卷脱机状态后，请联系相应的管理员或操作员以手动重新启动已关闭的节点并修复存储故障转移问题。

确定卷是否处于脱机状态，因为其 **SVM** 已在 **Active IQ Unified Manager** 中停止

您可以使用 Unified Manager Web UI 确认或排除这样一种可能性：卷脱机是因为其主机存储虚拟机（SVM）因托管该 SVM 根卷的节点停机而停止。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

要确定卷脱机状态是否是由于托管该 SVM 根卷的节点停机而导致其主机 SVM 停止所引起的，请执行以下操作：

步骤

1. 在离线卷的 **Volume / Health** 详细信息页面的 **Related Devices** 窗格中找到并单击 SVM 下显示的超文本链接。

   Storage VM / 运行状况详细信息页面显示托管 SVM 的 “running” 或 “stopped” 状态。如果 SVM 状态为运行，则卷离线状态不是由托管该 SVM 根卷的节点关闭引起的。

2. 如果 SVM 状态为已停止，则单击 查看 **SVM** 以进一步确定托管 SVM 停止的原因。
3. 在 **Health: All Storage VMs** 视图的 SVM 列标题上，单击筛选器符号 ，然后键入已停止的 SVM 的名

称。

该 SVM 的信息显示在表中。

4. 在 **Health: All Storage VMs** 视图中，单击 ，然后选择 **Root Volume** 选项。

根卷列将添加到 SVM 清单中，并显示已停止 SVM 的根卷的名称。

5. 在根卷列中，单击根卷的名称以显示该卷的 **Storage VM /** 运行状况 详细信息页面。

如果 SVM 根卷的状态为（在线），则原始卷离线的原因不是托管该 SVM 根卷的节点已停机。

6. 如果 SVM 根卷的状态为（离线），则在 SVM 根卷的卷/运行状况详细信息页面的“相关设备”窗格中找到并单击显示在“聚合”下的超文本链接。
7. 在聚合的*聚合/健康*详细信息页面的*相关设备*窗格中找到并单击节点下显示的超文本链接。

群集/运行状况详细信息页面上的节点选项卡显示 SVM 根卷托管节点所属的 HA 节点对的状态。显示屏上显示了节点的状态。

在确认卷脱机状态是由该卷的主机 SVM 脱机状态引起的（这本身是由托管该 SVM 根卷的节点停机引起的）后，请联系相应的管理员或操作员手动重新启动停机的节点。

确定卷是否因 **Active IQ Unified Manager** 中的磁盘损坏而脱机

您可以使用 Unified Manager Web UI 确认或排除卷脱机是由于 RAID 磁盘问题导致其主机聚合脱机这一可能性。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

要确定卷脱机状态是否由使托管聚合脱机的 RAID 磁盘问题引起，请执行以下操作：

步骤

1. 在 **Volume / Health** 详细信息页面的 **Related Devices** 窗格中找到并单击显示在 Aggregate 下的超文本链接。

聚合/运行状况详细信息页面显示托管聚合的联机或脱机状态。如果聚合状态为联机，则 RAID 磁盘问题不是卷脱机的原因。

2. 如果聚合状态为离线，则单击*磁盘信息*，并在*磁盘信息*选项卡上的*事件*列表中查找损坏的磁盘事件。
3. 要进一步识别损坏的磁盘，请单击 相关设备 窗格中节点下方显示的超文本链接。

此时将显示集群/健康详细信息页面。

4. 单击*磁盘*，然后在*过滤器*窗格中选择*已损坏*，以列出所有处于损坏状态的磁盘。

如果处于故障状态的磁盘导致主机聚合处于离线状态，则聚合的名称将显示在“受影响的聚合”列中。

在确认卷离线状态是由 RAID 磁盘损坏以及随之而来的离线主机聚合引起之后，请联系相应的管理员或操作员手动更换损坏的磁盘，并使聚合恢复联机。

解决容量问题

解决 **Active IQ Unified Manager** 中的容量问题

此工作流程提供了如何解决容量问题的示例。在这种情况下，您是管理员或操作员，您可以访问 Unified ManagerDashboard 页面，查看是否有任何受监控的存储对象存在容量问题。您想确定问题的可能原因和解决方案。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

在“仪表板”页面上，您可以在“事件”下拉列表下的“容量”面板中查找“卷空间已满”错误事件。

步骤

1. 在 **Dashboard** 页面的 **Capacity** 面板中，单击 Volume Space Full 错误事件的名称。

   将显示该错误的事件详细信息页面。

2. 在*事件*详细信息页面中，您可以执行以下一项或多项任务：
   - 查看“原因”字段中的错误消息，然后单击“建议的补救措施”下的建议，以查看可能的补救措施说明。
   - 单击“源”字段中的对象名称（在本例中为卷）以获取有关对象的详细信息。
   - 查找可能已添加的有关此事件的备注。
   - 为事件添加备注。
   - 将此事件分配给另一个用户。
   - 请确认此事件。
   - 将该事件标记为已解决。

相关信息

"事件详细信息页面"

在 **Active IQ Unified Manager** 中对卷已满问题执行建议的修复操作

收到“`Volume Space Full`”错误事件后，您查看事件详细信息页面上的建议补救措施，并决定执行其中一项建议操作。

开始之前

您必须具有应用程序管理员或存储管理员角色。

具有任何角色的用户都可以执行此工作流程中使用 Unified Manager 的所有任务。

在此示例中，您在 Unified ManagerEvent Management 清单页面上看到了“卷空间已满”错误事件，并单击了该事件的名称。

您可能对已满的卷执行的补救措施包括以下内容：

- 对卷启用自动增长、重复数据删除或压缩
- 调整大小或移动卷
- 从卷中删除或移动数据

虽然所有这些操作都必须从 ONTAP System Manager 或 ONTAP CLI 执行，但您可以使用 Unified Manager 查找您可能需要的信息，以确定要采取的操作。

步骤

1. 在*事件*详细信息页面中，单击源字段中的卷名称以查看有关受影响卷的详细信息。
2. 在*卷/运行状况*详细信息页面上，单击*配置*，看到卷上已启用重复数据删除和压缩。

   您决定调整此卷的大小。

3. 在*相关设备*窗格中，单击托管聚合的名称，以查看聚合是否可以容纳更大的卷。
4. 在*聚合/运行状况*详细信息页面上，您可以看到托管已满卷的聚合确实具有足够的未提交容量，因此您可以使用 ONTAP System Manager 调整卷的大小，从而为其提供更多容量。

相关信息

"事件详细信息页面"

管理运行状况阈值

了解 **Active IQ Unified Manager** 中的存储容量运行状况阈值

存储容量运行状况阈值是指 Unified Manager 服务器生成事件以报告存储对象任何容量问题的临界点。您可以配置警报，以便在发生此类事件时发送通知。

所有聚合、卷和 qtree 的存储容量运行状况阈值都设置为默认值。您可以根据需要更改对象或一组对象的设置。

配置全局运行状况阈值设置

在 **Active IQ Unified Manager** 中配置全局运行状况阈值设置

您可以为容量、增长、Snapshot 预留、配额和 inode 配置全局运行状况阈值条件，以有效监控您的聚合、卷和 qtree 大小。您还可以编辑用于生成超出延迟阈值的事件的设置。

全局运行状况阈值设置适用于与其关联的所有对象，例如聚合、卷等。当超过阈值时，将生成一个事件，如果配置了警报，将发送警报通知。阈值默认值设置为推荐值，但您可以修改它们以按一定时间间隔生成事件，从而满足您的特定需求。更改阈值时，将在下一个监控周期中生成或废弃事件。

可从左侧导航菜单的“事件阈值”部分访问全局运行状况阈值设置。您还可以从清单页面或该对象的详细信息页面修改单个对象的阈值设置。

- 有关信息，请参见 "配置全局聚合运行状况阈值"。

  您可以为所有聚合配置容量、增长和 Snapshot 副本的运行状况阈值设置，以跟踪任何阈值违规。

- 有关信息，请参见 "配置全局卷运行状况阈值"。

您可以编辑所有卷的容量、Snapshot 副本、qtree 配额、卷增长、覆盖预留空间和 inode 的健康阈值设置，以跟踪任何阈值违规。

- 有关信息，请参见 "配置全局 qtree 运行状况阈值"。

  您可以编辑所有 qtree 容量的运行状况阈值设置，以跟踪任何阈值违规。

- 有关信息，请参见 "编辑非受管保护关系的滞后运行状况阈值设置"。

  您可以增加或减少警告或错误延迟时间百分比，以便以更适合您需求的时间间隔生成事件。

在 **Active IQ Unified Manager** 中配置全局聚合运行状况阈值

您可以为所有聚合配置全局运行状况阈值，以跟踪任何阈值违规。系统会为阈值违规生成适当的事件，您可以根据这些事件采取预防措施。您可以根据适用于所有受监控聚合的阈值的最佳实践设置来配置全局值。

开始之前

您必须具有应用程序管理员或存储管理员角色。

全局配置选项时，将修改对象的默认值。但是，如果在对象级别更改了默认值，则不会修改全局值。

阈值选项具有用于更好地监控的默认值，但是，您可以更改这些值以满足您的环境要求。

当对驻留于聚合上的卷启用自动增长时，系统将根据自动增长设置的最大卷大小（而非原始卷大小）来评估是否超出聚合容量阈值。

健康阈值不适用于节点的根聚合。

步骤

1. 在左侧导航窗格中，单击*事件阈值* > 聚合。
2. 为容量、增长和 Snapshot 副本配置适当的阈值。
3. 单击 **Save**。

相关信息

"添加用户"

在 **Active IQ Unified Manager** 中配置全局卷运行状况阈值

您可以配置所有卷的全局运行状况阈值，以跟踪任何阈值违规情况。系统会针对运行状况阈值违规生成相应事件，您可以根据这些事件采取预防措施。您可以根据适用于所有受监控卷的阈值最佳实践设置来配置全局值。

开始之前

您必须具有应用程序管理员或存储管理员角色。

大多数阈值选项都有默认值，以便更好地进行监控。但是，您可以更改这些值以满足您的环境要求。

请注意，当在卷上启用 Autogrow 时，系统将根据 Autogrow 设置的最大卷大小（而不是基于原始卷大小）来判断容量阈值是否已超出。

> 默认值 1000 个 Snapshot 副本仅适用于 ONTAP 版本为 9.4 或更高版本时的 FlexVol 卷，以及 ONTAP 版本为 9.8 或更高版本时的 FlexGroup 卷。对于安装了较旧版本 ONTAP 软件的集群，每个卷的最大 Snapshot 副本数为 250 个。对于这些较旧版本，Unified Manager 会将 1000（以及 1000 到 250 之间的任何数字）解释为 250；这意味着当 Snapshot 副本数量达到 250 时，您将继续收到事件。如果您希望针对这些较旧版本将此阈值设置为低于 250，则必须在此处、在"运行状况: 所有卷"视图中或在"卷/运行状况详细信息"页面中将阈值设置为 250 或更低。

步骤

1. 在左侧导航窗格中，单击*事件阈值* > 卷。
2. 为容量、Snapshot 副本、qtree 配额、卷增长和 inode 配置适当的阈值。
3. 单击 **Save**。

相关信息

"添加用户"

在 **Active IQ Unified Manager** 中配置全局 **qtree** 运行状况阈值

您可以为所有 qtree 配置全局运行状况阈值，以跟踪任何阈值违规情况。系统会针对运行状况阈值违规生成相应事件，您可以根据这些事件采取预防措施。您可以根据适用于所有受监控 qtree 的阈值最佳实践设置来配置全局值。

开始之前

您必须具有应用程序管理员或存储管理员角色。

阈值选项具有用于更好地监控的默认值，但是，您可以更改这些值以满足您的环境要求。

仅当在 qtree 上设置了 Qtree 配额或默认配额时，才会为 qtree 生成事件。如果在用户配额或组配额中定义的空间超过阈值，则不会生成事件。

步骤

1. 在左侧导航窗格中，单击*事件阈值* > **Qtree**。
2. 配置适当的容量阈值。
3. 单击 **Save**。

在 **Active IQ Unified Manager** 中为非受管保护关系配置滞后阈值

您可以编辑非托管保护关系的全局默认延迟警告和错误运行状况阈值设置，以便按照适合您需要的时间间隔生成事件。

开始之前

您必须具有应用程序管理员或存储管理员角色。

滞后时间不得超过定义的传输计划间隔。例如，如果传输计划为每小时一次，则滞后时间不得超过一小时。滞后阈值指定了滞后时间不得超过的百分比。以一小时为例，如果滞后阈值定义为 150%，则当滞后时间超过 1.5 小

时时，您将收到一个事件。

此任务中描述的设置将全局应用于所有非托管保护关系。这些设置无法专门指定并仅应用于某一个非托管保护关系。

步骤

1. 在左侧导航窗格中，单击*事件阈值* > 关系。
2. 根据需要增加或减少全局默认警告或错误滞后时间百分比。
3. 要禁用从任何延迟阈值触发的警告或错误事件，请取消选中 已启用 旁边的复选框。
4. 单击 **Save**。

相关信息

"添加用户"

在 **Active IQ Unified Manager** 中编辑单个聚合运行状况阈值设置

您可以编辑一个或多个聚合的聚合容量、增长和 Snapshot 副本的运行状况阈值设置。超过阈值时，将生成警报，您将收到通知。这些通知可帮助您根据生成的事件采取预防措施。

开始之前

您必须具有应用程序管理员或存储管理员角色。

根据阈值更改，下一监控周期将生成或废弃事件。

当对驻留于聚合上的卷启用自动增长时，系统将根据自动增长设置的最大卷大小（而非原始卷大小）来评估是否超出聚合容量阈值。

步骤

1. 在左侧导航窗格中，单击*存储* > 聚合。
2. 在 运行状况：所有聚合 视图中，选择一个或多个聚合，然后单击 编辑阈值。
3. 在*编辑聚合阈值*对话框中，通过选中相应的复选框，然后修改设置来编辑以下选项之一的阈值设置：容量、增长或 Snapshot 副本。
4. 单击 **Save**。

相关信息

"添加用户"

在 **Active IQ Unified Manager** 中编辑单个卷的运行状况阈值设置

您可以编辑一个或多个卷的卷容量、增长、配额和空间保留的运行状况阈值设置。当超过阈值时，将生成警报，您将收到通知。这些通知可帮助您根据生成的事件采取预防措施。

开始之前

您必须具有应用程序管理员或存储管理员角色。

根据阈值更改，下一监控周期将生成或废弃事件。

请注意，当在卷上启用 Autogrow 时，系统将根据 Autogrow 设置的最大卷大小（而不是基于原始卷大小）来判断容量阈值是否已超出。

> 默认值 1000 个 Snapshot 副本仅适用于 ONTAP 版本为 9.4 或更高版本时的 FlexVol 卷，以及 ONTAP 版本为 9.8 或更高版本时的 FlexGroup 卷。对于安装了较旧版本 ONTAP 软件的集群，每个卷的最大 Snapshot 副本数为 250 个。对于这些较旧版本，Unified Manager 会将 1000（以及 1000 到 250 之间的任何数字）解释为 250；这意味着当 Snapshot 副本数量达到 250 时，您将继续收到事件。如果您希望针对这些较旧版本将此阈值设置为低于 250，则必须在此处、在"运行状况: 所有卷"视图中或在"卷/运行状况详细信息"页面中将阈值设置为 250 或更低。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在*运行状况：所有卷*视图中，选择一个或多个卷，然后单击*编辑阈值*。
3. 在*编辑卷阈值*对话框中，通过选中相应的复选框，然后修改设置来编辑以下选项之一的阈值设置：容量、Snapshot 副本、qtree 配额、增长或 inode。
4. 单击 **Save**。

相关信息

"添加用户"

在 **Active IQ Unified Manager** 中编辑单个 **qtree** 运行状况阈值设置

您可以编辑一个或多个 qtree 的 qtree 容量的运行状况阈值设置。当超过阈值时，将生成警报，您将收到通知。这些通知可帮助您根据生成的事件采取预防措施。

开始之前

您必须具有应用程序管理员或存储管理员角色。

根据阈值更改，下一监控周期将生成或废弃事件。

步骤

1. 在左侧导航窗格中，单击 存储 > **Qtrees**。
2. 在*容量：所有 Qtree*视图中，选择一个或多个 qtree，然后单击*编辑阈值*。
3. 在*编辑 Qtree 阈值*对话框中，更改所选 qtree 的容量阈值，然后单击*保存*。

> 您还可以从 Storage VM / Health 详细信息页面的 Qtrees 选项卡中设置单个 qtree 阈值。

管理集群安全目标

在 **Active IQ Unified Manager** 中管理集群安全目标

Unified Manager 提供了一个仪表板，用于根据 *NetApp Security Hardening Guide for ONTAP 9* 中定义的建议，确定您的 ONTAP 集群、存储虚拟机（SVM）和卷的安全程度。

安全控制面板的目标是显示您的 ONTAP 集群与 NetApp 建议指南不一致的任何区域，以便您可以解决这些潜在问题。在大多数情况下，您可以使用 ONTAP System Manager 或 ONTAP CLI 解决问题。您的组织可能不会遵循所有建议，因此在某些情况下，您无需进行任何更改。

有关详细建议和解决方法，请参见 "适用于 ONTAP 9 的 NetApp 安全强化指南"（TR-4569）。

除了报告安全状态之外，Unified Manager 还会为存在安全违规的任何群集或 SVM 生成安全事件。您可以在“事件管理清单”页面中跟踪这些问题，还可以为这些事件配置警报，以便在发生新安全事件时通知存储管理员。

有关详细信息，请参见"正在评估哪些安全标准"。

评估的安全条件

了解 **Active IQ Unified Manager** 如何评估安全标准

一般来说，将根据 *NetApp Security Hardening Guide for ONTAP 9* 中定义的建议评估您的 ONTAP 集群、存储虚拟机（SVM）和卷的安全标准。

其中一些安全检查包括：

- 集群是否正在使用安全身份验证方法，例如 SAML
- 对等集群的通信是否已加密
- storage VM 是否已启用其审核日志
- 您的卷是否启用了软件或硬件加密

有关详细信息，请参见有关合规类别和 "适用于 ONTAP 9 的 NetApp 安全强化指南"的主题。

> 从 Active IQ 平台报告的升级事件也被视为安全事件。这些事件指出了需要升级 ONTAP 软件、节点固件或操作系统软件（针对安全公告）才能解决的问题。这些事件不会显示在安全面板中，但可以从事件管理清单页面中获取。

有关详细信息，请参见"管理集群安全目标"。

了解 **Active IQ Unified Manager** 中的集群合规性类别

此表描述了 Unified Manager 评估的集群安全合规性参数、NetApp 建议，以及该参数是否影响集群合规或不合规的整体判定。

在集群上具有不合规的 SVM 将影响集群的合规值。因此，在某些情况下，在集群安全被视为合规之前，您可能需要解决 SVM 的安全问题。

请注意，并非所有安装都会显示下面列出的所有参数。例如，如果没有对等群集，或者在群集上禁用了 AutoSupport，则不会在 UI 页面中看到群集对等或 AutoSupport HTTPS 传输项目。

参数	问题描述	建议	影响集群合规性
全局 FIPS	指示是否启用或禁用全球 FIPS（联邦信息处理标准）140-2 合规模式。启用 FIPS 后，TLSv1 和 SSLv3 将被禁用，只允许 TLSv1.1 和 TLSv1.2。	已启用	是
Telnet	指示对系统的 Telnet 访问是启用还是禁用。NetApp 建议使用安全 Shell（SSH）进行安全远程访问。	已禁用	是
不安全 SSH 设置	指示 SSH 是否使用不安全密码，例如以 *cbc 开头的密码。	否	是
登录横幅	指示是否为访问系统的用户启用或禁用登录横幅。	已启用	是
创建集群对等关系	指示对等集群之间的通信是加密还是未加密。必须在源和目标集群上配置加密，才能将此参数视为合规。	已加密	是
网络时间协议	指示集群是否具有一个或多个配置的 NTP 服务器。为了保证冗余和最佳服务，NetApp 建议至少将三个 NTP 服务器与集群相关联。	已配置	是
OCSP	从 9.14.1 开始，Active IQ Unified Manager 在 Storage Virtual Machine（SVM，以前称为 Vserver）级别提供在线证书状态协议（OCSP）状态信息。这意味着 OCSP 验证将应用于与 SVM 建立的所有 SSL/TLS 连接，并确保这些连接中使用的证书的完整性和有效性。	已启用	否
远程审核日志记录	指示日志转发（Syslog）是否已加密。	已加密	是
AutoSupport HTTPS 传输	指示是否使用 HTTPS 作为默认传输协议，用于向 NetApp 支持发送 AutoSupport 消息。	已启用	是

参数	问题描述	建议	影响集群合规性
默认管理员用户	指示是否启用或禁用默认管理员用户（内置）。NetApp 建议锁定（禁用）任何不需要的内置帐户。	已禁用	是
SAML 用户	指示是否配置了 SAML。通过 SAML，您可以将多因素身份验证（MFA）配置为单点登录的登录方法。	否	否
Active Directory 用户	指示是否配置了 Active Directory。Active Directory 和 LDAP 是用户访问集群的首选身份验证机制。	否	否
LDAP 用户	指示是否配置了 LDAP。相比本地用户，Active Directory 和 LDAP 是管理集群的用户首选的身份验证机制。	否	否
证书用户	指示是否已将证书用户配置为登录到集群。	否	否
本地用户	指示是否将本地用户配置为登录到集群。	否	否
远程 Shell	指示是否启用了 RSH。出于安全原因，应禁用 RSH。首选用于安全远程访问的 Secure Shell (SSH)。	已禁用	是
MD5 正在使用	指示 ONTAP 用户帐户是否使用不太安全的 MD5 哈希函数。最好将 MD5 哈希用户帐户迁移到更安全的加密哈希函数，如 SHA-512。	否	是
证书颁发者类型	指示使用的数字证书的类型。	CA 签名	否

了解 **Active IQ Unified Manager** 中的 **Storage VM** 合规性类别

此表描述了 Unified Manager 评估的 Storage Virtual Machine (SVM) 安全合规性标准、NetApp 建议，以及该参数是否影响对 SVM 合规或不合规的整体判定。

参数	问题描述	建议	影响 **SVM** 合规性
审核日志	指示是否启用或禁用审核日志记录。	已启用	是

参数	问题描述	建议	影响 **SVM** 合规性
不安全 SSH 设置	指示 SSH 是否使用不安全的密码，例如以 `cbc*`开头的密码。	否	是
登录横幅	指示用户访问系统上的 SVM 时，登录横幅是否已启用或禁用。	已启用	是
LDAP 加密	指示 LDAP 加密是否已启用或禁用。	已启用	否
NTLM 身份验证	指示 NTLM 身份验证是否已启用或禁用。	已启用	否
LDAP 负载签名	指示是启用还是禁用 LDAP 负载签名。	已启用	否
CHAP 设置	指示 CHAP 是启用还是禁用。	已启用	否
Kerberos V5	指示是启用还是禁用 Kerberos V5 身份验证。	已启用	否
NIS 身份验证	指示是否配置了使用 NIS 身份验证。	已禁用	否
FPolicy 状态活动	指示是否已创建 FPolicy。	是	否
已启用 SMB 加密	指示是否未启用 SMB - 签名和密封。	是	否
已启用 SMB 签名	指示是否未启用 SMB - 签名。	是	否

了解 **Active IQ Unified Manager** 中的卷合规性类别

此表描述了 Unified Manager 评估的卷加密参数，以确定卷上的数据是否得到充分保护，防止未经授权的用户访问。

请注意，卷加密参数不影响集群或存储 VM 是否被视为合规。

参数	问题描述
软件加密	显示使用 NetApp 卷加密（NVE）或 NetApp 聚合加密（NAE）软件加密解决方案保护的卷数。
硬件加密	显示使用 NetApp 存储加密（NSE）硬件加密保护的卷数。
软件加密和硬件加密	显示受软件和硬件加密保护的卷数。
未加密	显示未加密的卷数。

了解 **Active IQ Unified Manager** 中的集群和 **SVM** 合规性状态

如果不符合根据 *NetApp Security Hardening Guide for ONTAP 9* 中定义的建议评估的任一安全条件，则集群和 Storage Virtual Machine (SVM) 将视为不合规。此外，如果任何

SVM 标记为不合规，则集群将视为不合规。

安全卡中的状态图标相对于其合规性具有下列含义：

- - 参数按建议配置。
- - 未按建议配置参数。
- - 此功能未在集群上启用，或此参数未按建议配置，但此参数不会影响对象的合规性。

请注意，卷加密状态与集群或 SVM 是否合规无关。

在 **Active IQ Unified Manager** 中查看集群和 **Storage VM** 的安全状态

Active IQ Unified Manager 允许您从界面中的不同点查看环境中存储对象的安全状态。您可以根据定义的参数收集和分析信息和报告，并检测受监控集群和存储虚拟机上的可疑行为或未经授权的系统更改。

有关安全建议，请参见 "适用于 ONTAP 9 的 NetApp 安全强化指南"

在安全页面上查看对象级安全状态

作为系统管理员，您可以使用 安全 页面了解您的 ONTAP 集群和存储虚拟机在数据中心和站点级别的安全强度。支持的对象是集群、存储虚拟机和卷。请按照以下步骤操作：

步骤

1. 在左侧导航窗格中，单击*仪表板*。
2. 根据您是要查看所有受监控集群还是单个集群的安全状态，选择 所有集群 或从下拉菜单中选择单个集群。
3. 单击*安全*面板中的右箭头。此时将显示“安全”页面。

单击条形图、计数和 `View Reports`链接将转到卷、群集或 Storage VM 页面，以便您根据需要查看相应的详细信息或生成报告。

安全页面显示以下面板：

- 集群合规性：数据中心中所有集群的安全状态（合规或不合规的集群数量）
- 存储虚拟机合规性：数据中心中所有存储虚拟机的安全状态（合规或不合规的存储虚拟机数量）
- 卷加密：环境中所有卷的卷加密状态（已加密或未加密的卷数量）
- 卷反勒索软件状态：环境中所有卷的安全状态（启用或禁用反勒索软件的卷数）
- 集群身份验证和证书：使用每种身份验证方法（如 SAML、Active Directory 或通过证书和本地身份验证）的集群数量。该面板还显示证书已过期或将在 60 天内过期的集群数量。

在集群页面上查看所有集群的安全详细信息

*集群/安全*详细信息页面使您能够查看集群级别的安全合规性状态。

步骤

1. 在左侧导航窗格中，单击*存储 > 群集*。

2. 选择 查看 > 安全 > 所有集群。

将显示默认安全参数，例如全局 FIPS、Telnet、不安全的 SSH 设置、登录横幅、网络时间协议、AutoSupport HTTPS 传输以及集群证书过期状态。

您可以单击⋮更多选项按钮，并选择在 Unified Manager 的*安全*页面或 System Manager 上查看安全详细信息。您应该拥有有效的凭据才能在 System Manager 上查看详细信息。

> 如果集群的证书已过期，您可以单击 **Cluster Certificate Validity** 下的 `expired`，然后从 System Manager（9.10.1 及更高版本）续订。如果 System Manager 实例的版本早于 9.10.1，则无法单击 `expired`。

从 **Storage VMs** 页面查看所有集群的安全详细信息

可使用 存储 **VM /** 安全 详细信息页面查看存储 VM 级别的安全合规性状态。

步骤

1. 在左侧导航窗格中，单击 **Storage > Storage VMs**。
2. 选择 查看 **>** 安全 **>** 所有 **Storage VM**。此时将显示包含安全参数的集群列表。

您可以通过检查安全参数（例如存储 VM、集群、登录横幅、审计日志和不安全的 SSH 设置）来默认查看存储 VM 的安全合规性。

您可以单击⋮更多选项按钮，并选择在 Unified Manager 的*安全*页面或 System Manager 上查看安全详细信息。您应该拥有有效的凭据才能在 System Manager 上查看详细信息。

有关卷和存储 VM 的反勒索软件安全详细信息，请参见 "查看所有卷和 Storage VM 的反勒索软件状态"。

查看 **Active IQ Unified Manager** 中可能需要软件或固件更新的安全事件

某些安全事件的影响区域为“`Upgrade`”。这些事件由 Active IQ 平台报告，它们指出的问题需要您通过升级 ONTAP 软件、节点固件或操作系统软件（针对安全公告）来解决。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

您可能需要立即对其中一些问题执行纠正措施，而其他问题可能要等到下一次定期维护时才能解决。您可以查看所有这些事件，并将其分配给可以解决问题的用户。此外，如果存在某些您不希望收到通知的安全升级事件，此列表可以帮助您识别这些事件，以便您可以将其禁用。

步骤

1. 在左侧导航窗格中，单击*事件管理*。

   默认情况下，所有活动（新建和已确认）事件都将显示在事件管理清单页面上。

2. 在“视图”菜单中，选择 升级事件。

   此页面显示所有活动升级安全事件。

查看集群如何在 **Active IQ Unified Manager** 中的所有集群上管理用户身份验证

安全页面显示用于对每个群集上的用户进行身份验证的身份验证类型，以及使用每种类型访问群集的用户数。这使您能够验证是否按照组织的定义安全地执行用户身份验证。

步骤

1. 在左侧导航窗格中，单击*仪表板*。
2. 在仪表板的顶部，从下拉菜单中选择*所有集群*。
3. 单击*安全*面板中的右箭头，将显示*安全*页面。
4. 查看*集群身份验证*卡，查看使用每种身份验证类型访问系统的用户数量。
5. 查看*集群安全*卡以查看用于对每个集群上的用户进行身份验证的身份验证机制。

如果有一些用户使用不安全的方法或 NetApp 不推荐的方法访问系统，您可以禁用该方法。

查看 **Active IQ Unified Manager** 中所有卷的加密状态

您可以查看所有卷及其当前加密状态的列表，以便确定卷上的数据是否受到充分保护，防止未经授权的用户访问。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

可以应用于卷的加密类型包括：

- 软件 — 使用 NetApp 卷加密 (NetApp Volume Encryption, NVE) 或 NetApp 聚合加密 (NetApp Aggregate Encryption, NAE) 软件加密解决方案进行保护的卷。
- 硬件 — 使用 NetApp 存储加密 (NetApp Storage Encryption, NSE) 硬件加密进行保护的卷。
- 软件和硬件 — 同时使用软件和硬件加密进行保护的卷。
- 无 — 未加密的卷。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在 View 菜单中，选择 **Health** > **Volumes Encryption**
3. 在*运行状况：卷加密*视图中，对*加密类型*字段进行排序，或使用筛选器显示具有特定加密类型或未加密的卷（加密类型为 “None”）。

查看 **Active IQ Unified Manager** 中所有卷和存储 **VM** 的反勒索软件状态

您可以查看所有卷和存储虚拟机（SVM）的列表及其当前反勒索软件状态，以便确定卷和 SVM 上的数据是否受到充分保护，免受勒索软件攻击。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

有关不同反勒索软件状态的更多信息，请参见 "ONTAP：启用反勒索软件"。

查看具有反勒索软件检测功能的所有卷的安全详细信息

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在“视图”菜单中，选择 运行状况 > 安全 > 防勒索软件
3. 在*安全：反勒索软件*视图中，您可以按各个字段排序或使用筛选器。

> 离线卷、受限卷、SnapLock 卷、FlexGroup 卷、FlexCache 卷、仅 SAN 卷、已停止存储虚拟机的卷、存储虚拟机的根卷或数据保护卷不支持反勒索软件。

查看具有反勒索软件检测功能的所有 **Storage VM** 的安全详细信息

步骤

1. 在左侧导航窗格中，单击 **Storage > Storage VMs**。
2. 选择 查看 **>** 安全 **>** 反勒索软件。此时将显示具有反勒索软件状态的 SVM 列表。

> 未启用 NAS 协议的存储 VM 不支持防勒索软件监控。

查看 **Active IQ Unified Manager** 中的所有活动安全事件

您可以查看所有活动的安全事件，然后将每个事件分配给可以解决此问题的用户。此外，如果您不希望接收某些安全事件，此列表可帮助您确定要禁用的事件。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*事件管理*。

   默认情况下，“新建”和“已确认”事件将显示在“事件管理”清单页面上。

2. 在“视图”菜单中，选择 活动安全事件。

   该页面显示过去 7 天生成的所有新建和已确认的安全事件。

在 **Active IQ Unified Manager** 中添加安全事件警报

您可以为单个安全事件配置警报，就像 Unified Manager 接收的任何其他事件一样。此外，如果您希望以相同方式处理所有安全事件，并将电子邮件发送给同一个人，则可以创建单个警报，以便在触发任何安全事件时通知您。

开始之前

您必须具有应用程序管理员或存储管理员角色。

下面的示例演示如何为“`Telnet Protocol Enabled`”安全事件创建警报。如果将 Telnet 访问配置为对集群进行远程管理访问，这将发送警报。您可以使用相同的方法为所有安全事件创建警报。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。
2. 在*警报设置*页面中，单击*添加*。
3. 在*添加警报*对话框中，单击*名称*，并输入警报的名称和描述。
4. 单击*资源*并选择要启用此警报的集群或集群。
5. 单击 事件 并执行以下操作：
   a. 在事件严重程度列表中，选择*警告*。
   b. 在匹配事件列表中，选择 **Telnet Protocol Enabled**。
6. 单击*操作*，然后在*提醒这些用户*字段中选择将接收警报电子邮件的用户的名称。
7. 在此页面上配置有关通知频率、发出 SNMP 陷阱和执行脚本的任何其他选项。
8. 单击 **Save**。

在 **Active IQ Unified Manager** 中禁用特定安全事件

默认情况下，所有事件均处于启用状态。您可以禁用特定事件，以防止为环境中不重要的事件生成通知。如果您希望恢复接收有关这些事件的通知，可以启用已禁用的事件。

开始之前

您必须具有应用程序管理员或存储管理员角色。

禁用事件时，系统中以前生成的事件将被标记为已废弃，并且不会触发为这些事件配置的警报。启用已禁用的事件后，将从下一监控周期开始生成这些事件的通知。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 事件设置。
2. 在*事件*设置页面中，通过选择以下选项之一禁用或启用事件：

目的	操作
禁用事件	a. 单击 **Disable**。 b. 在禁用事件对话框中，选择*警告*严重性。这是所有安全事件的类别。 c. 在匹配事件列中，选择要禁用的安全事件，然后单击右箭头将这些事件移动到禁用事件列。 d. 单击*保存并关闭*。 e. 验证已禁用的事件是否显示在“事件设置”页面的列表视图中。
启用事件	a. 从禁用事件列表中，选中要重新启用的事件的复选框。 b. 单击 启用。

在 **Active IQ Unified Manager** 中查看安全事件

安全事件根据 *NetApp Security Hardening Guide for ONTAP 9* 中定义的参数，为您提供有关 ONTAP 集群、存储虚拟机（SVM）和卷的安全状态信息。这些事件会通知您潜在的问题，以便您评估其严重程度，并在必要时解决问题。

安全事件按源类型分组，包括事件和陷阱名称、影响级别和严重程度。这些事件出现在集群和存储 VM 事件类别中。

管理备份和还原操作

在 **Active IQ Unified Manager** 中管理备份和还原操作

您可以创建 Active IQ Unified Manager 的备份，并使用还原功能将备份还原到同一（本地）系统或新的（远程）系统，以防发生系统故障或数据丢失。

有三种备份和还原方法，具体取决于已安装 Unified Manager 的操作系统，以及要管理的群集和节点的数量：

操作系统	部署规模	建议的备份方法
VMware vSphere	任意	Unified Manager 虚拟设备的 VMware 快照
Red Hat Enterprise Linux	小型	Unified Manager MySQL 数据库转储
	大型	Unified Manager 数据库的 NetApp 快照
Microsoft Windows	小型	Unified Manager MySQL 数据库转储
	大型	使用 iSCSI 协议的 Unified Manager 数据库的 NetApp 快照

下面几节将介绍这些不同的方法。

在虚拟设备上备份和恢复 **Active IQ Unified Manager**

当安装在虚拟设备上时，Unified Manager 的备份和还原模式是捕获和还原完整虚拟应用程序的映像。

通过下列任务可以完成虚拟设备的备份：

1. 关闭虚拟机并获取 Unified Manager 虚拟设备的 VMware 快照。
2. 在数据存储上创建 NetApp Snapshot 副本以捕获 VMware 快照。

   如果此数据存储库未托管在运行 ONTAP 软件的系统上，请按照存储供应商准则来为 VMware 快照创建备份。

3. 将 NetApp Snapshot 副本或 Snapshot 等效副本复制到备用存储。
4. 删除 VMware 快照。

您应该使用这些任务实施备份计划，以确保在出现问题时对 Unified Manager 虚拟设备进行保护。

要还原虚拟机，可以使用所创建的 VMware 快照将虚拟机还原到备份时间点状况。

使用 **MySQL** 数据库转储进行备份和还原

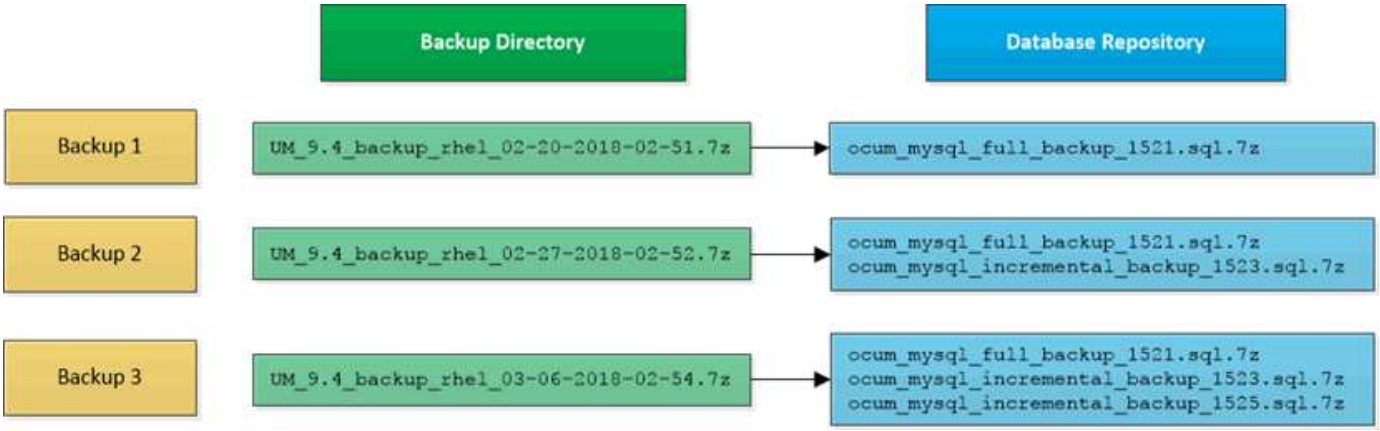
使用 **Active IQ Unified Manager** 中的 **MySQL** 数据库转储进行备份和还原

MySQL 数据库转储备份是 Active IQ Unified Manager 数据库和配置文件的副本，可在系统故障或数据丢失时使用。您可以安排将备份写入本地目标或远程目标。强烈建议您定义 Active IQ Unified Manager 主机系统外部的远程位置。

当在 Linux 和 Windows 服务器上安装 Unified Manager 时，MySQL 数据库转储是默认的备份机制。但是，如果 Unified Manager 管理大量集群和节点，或者您的 MySQL 备份需要花费数小时才能完成，则可以使用 Snapshot 副本进行备份。此功能在 Red Hat Enterprise Linux 和 Windows 上可用。

数据库转储备份由备份目录中的单个文件和数据库存储库目录中的一个或多个文件组成。备份目录中的文件非常小，因为它只包含指向数据库存储库目录中重新创建备份所需的文件的指针。

首次生成数据库备份时，会在备份目录中创建一个文件，并在数据库存储库目录中创建一个完整备份文件。下次生成备份时，将在备份目录中创建一个文件，并在数据库存储库目录中创建一个增量备份文件，其中包含与完整备份文件的差异。随着您创建更多备份，此过程将继续进行，直到达到最大保留设置，如下图所示。



请勿重命名或删除这两个目录中的任何备份文件，否则后续的还原操作将会失败。

如果您将备份文件写入本地系统，则应启动一个进程将备份文件复制到远程位置，以便能够在出现需要完整还原的系统问题时使用这些文件。

在开始备份操作之前，Active IQ Unified Manager 会执行完整性检查，以验证所有必需的备份文件和备份目录是否存在且可写。它还会检查系统上是否有足够的空间来创建备份文件。

在 **Active IQ Unified Manager** 中配置数据库转储备份设置

您可以配置 Unified Manager 数据库转储备份设置，以设置数据库备份路径、保留计数和备份计划。您可以启用每日或每周计划备份。默认情况下，计划备份已禁用，但您应设置备份计划。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 在定义为备份路径的位置中，必须至少有 150 GB 的可用空间。

  建议您使用 Unified Manager 主机系统外部的远程位置。

- 在 Linux 系统上安装 Unified Manager 并使用 MySQL 备份时，请确保在备份目录上设置了以下权限和所有权。

  权限：0750，所有权：jboss:maintenance

- 在 Windows 系统上安装 Unified Manager 并使用 MySQL 备份时，请确保只有管理员可以访问备份目录。

首次执行备份所需的时间比后续备份所需的时间更长，因为第一次备份是完整备份。完整备份可能超过 1 GB，可能需要花费三到四个小时。后续备份是增量备份，需要的时间较少。

- 如果您发现增量备份文件的数量对于为备份分配的空间来说太大，则可以定期进行完整备份以替换旧备份及其增量文件。作为另一个选项，您可以使用 Snapshot 副本进行备份。
- 在新集群添加的最初 15 天内进行的备份可能不够准确，无法获取历史性能数据。

步骤

1. 在左侧导航窗格中，单击 常规 > 数据库备份。
2. 在*数据库备份*页面中，单击*备份设置*。
3. 为备份路径、保留计数和计划配置适当的值。

   保留数量的默认值为 10；您可以使用 0 来创建无限备份。

4. 选择*每日计划*或*每周计划*按钮，然后指定计划详细信息。
5. 单击*应用*。

将根据计划创建数据库转储备份文件。您可以在“数据库备份”页面中查看可用的备份文件。

了解 **Active IQ Unified Manager** 中的数据库还原

MySQL 数据库还原是将现有 Unified Manager 备份文件还原到同一台或不同 Unified Manager 服务器的过程。您可以从 Unified Manager 维护控制台执行还原操作。

如果要在同一（本地）系统上执行还原操作，并且备份文件都存储在本地，则可以使用默认位置运行还原选项。如果要在其他 Unified Manager 系统（远程系统）上执行还原操作，则必须先将备份文件从辅助存储复制到本地磁盘，然后才能运行还原选项。

在还原过程中，您将退出 Unified Manager。还原过程完成后，您可以登录到系统。

如果要将备份映像还原到新服务器，则在还原操作完成后，需要生成新的 HTTPS 安全证书并重新启动 Unified Manager 服务器。将备份映像还原到新服务器时，如果需要，还需要重新配置 SAML 身份验证设置。

在将 Unified Manager 升级到较新版本的软件后，旧备份文件无法用于还原映像。为了节省空间，升级 Unified Manager 时会自动删除除最新文件以外的所有旧备份文件。

相关信息

"生成 HTTPS 安全证书"

"启用 SAML 身份验证"

"通过 Active Directory 或 OpenLDAP 执行的身份验证"

在 **Linux** 系统上的 **Active IQ Unified Manager** 中还原 **MySQL** 数据库备份

如果发生数据丢失或数据损坏，您可以将 Unified Manager 恢复到以前的稳定状态，并将数据丢失降到最低。您可以使用 Unified Manager 维护控制台将 Unified Manager 数据库恢复到本地或远程 Red Hat Enterprise Linux 系统。

开始之前

- 您必须具有安装了 Unified Manager 的 Linux 主机的 root 用户凭据。
- 您必须拥有已授权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。
- 必须已将 Unified Manager 备份文件和数据库存储库目录的内容复制到要执行还原操作的系统上。

  建议将备份文件复制到默认目录 `/data/ocum-backup`。数据库存储库文件必须复制到 `/database-dumps-repo` 目录下的 `/ocum-backup` 子目录中。

- 备份文件必须为 `.7z`类型。

还原功能特定于平台和版本。您只能在相同版本的 Unified Manager 上还原 Unified Manager 备份。您可以将 Linux 备份文件或虚拟设备备份文件还原到 Red Hat Enterprise Linux 系统。

如果备份文件夹名称包含空格，则必须将绝对路径或相对路径包含在双引号中。

步骤

1. 如果要对新服务器执行还原，在安装 Unified Manager 后，请不要在安装完成后启动 UI 或配置任何集群、用户或身份验证设置。在还原过程中，备份文件会填充这些信息。
2. 使用 Secure Shell，连接到 Unified Manager 系统的 IP 地址或完全限定域名。
3. 使用维护用户 (umadmin) 名称和密码登录到此系统。
4. 输入命令 `maintenance_console`并按 Enter 键。
5. 在维护控制台*主菜单*中，输入*备份还原*选项的编号。
6. 输入 **Restore MySQL Backup** 的编号。
7. 出现提示时，输入备份文件的绝对路径。

   ```
   Bundle to restore from: /data/ocum-
   backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
   ```

   还原操作完成后，您可以登录到 Unified Manager。

恢复备份后，如果 OnCommand Workflow Automation 服务器无法正常工作，请执行以下步骤：

1. 在 Workflow Automation 服务器上，更改 Unified Manager 服务器的 IP 地址以指向最新的计算机。
2. 如果在步骤 1 中采集失败，请在 Unified Manager 服务器上重置数据库密码。

在 **Active IQ Unified Manager** 中还原 **Windows** 上的 **MySQL** 数据库备份

如果发生数据丢失或数据损坏，您可以使用恢复功能将 Unified Manager 恢复到以前的稳定状态，从而将损失降至最低。您可以使用 Unified Manager 维护控制台将 Unified Manager MySQL 数据库还原到本地 Windows 系统或远程 Windows 系统。

开始之前

- 您必须具有 Windows 管理员权限。
- 必须已将 Unified Manager 备份文件和数据库存储库目录的内容复制到要执行还原操作的系统上。

  建议将备份文件复制到默认目录 `\ProgramData\NetApp\OnCommandAppData\ocum\backup`。数据库存储库文件必须复制到 `\backup` 目录下的 `\database_dumps_repo` 子目录中。

- 备份文件必须为 `.7z`类型。

还原功能特定于平台和版本。只能在相同版本的 Unified Manager 上还原 Unified Manager MySQL 备份，并且 Windows 备份只能在 Windows 平台上还原。



如果文件夹名称包含空格，则必须将备份文件的绝对路径或相对路径包含在双引号中。

步骤

1. 如果要对新服务器执行还原，在安装 Unified Manager 后，请不要在安装完成后启动 UI 或配置任何集群、用户或身份验证设置。在还原过程中，备份文件会填充这些信息。
2. 使用管理员凭据登录到 Unified Manager 系统。
3. 以 Windows 管理员身份启动 PowerShell 或命令提示符。
4. 输入命令 `maintenance_console`并按 Enter 键。
5. 在维护控制台*主菜单*中，输入*备份还原*选项的编号。
6. 输入 **Restore MySQL Backup** 的编号。
7. 出现提示时，输入备份文件的绝对路径。

   ```
   Bundle to restore from:
   \ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac
   kup_windows_02-20-2020-02-51.7z
   ```

   还原操作完成后，您可以登录到 Unified Manager。

恢复备份后，如果 OnCommand Workflow Automation 服务器无法正常工作，请执行以下步骤：

1. 在 Workflow Automation 服务器上，更改 Unified Manager 服务器的 IP 地址以指向最新的计算机。
2. 如果在步骤 1 中采集失败，请在 Unified Manager 服务器上重置数据库密码。

使用 NetApp 快照进行备份和还原

在 Active IQ Unified Manager 中使用 NetApp 快照进行备份和恢复

NetApp Snapshot 副本创建 Unified Manager 数据库和配置文件的时间点映像，您可以使用该映像在系统故障或数据丢失时进行还原。您计划将 Snapshot 副本定期写入 ONTAP 群集之一上的卷，以便始终拥有当前副本。

此功能不适用于安装在虚拟设备上的 Active IQ Unified Manager。

在 Active IQ Unified Manager 中配置 Linux 备份

如果您的 Active IQ Unified Manager 安装在 Linux 计算机上，则可以决定使用 NetApp 快照配置备份和还原。

快照副本只需很少的时间，通常只需几分钟，而 Unified Manager 数据库的锁定时间也很短，因此您的安装几乎不会中断。映像占用的存储空间极小，性能开销可以忽略不计，因为它仅记录自上次创建快照副本以来对文件的更改。由于快照是在 ONTAP 集群上创建的，因此如果需要，您可以利用其他 NetApp 功能（例如 SnapMirror）来创建二级保护。

在开始备份操作之前，Unified Manager 会执行完整性检查以验证目标系统是否可用。

- 您只能在相同版本的 Active IQ Unified Manager 上还原 Snapshot 副本。

  例如，如果在 Unified Manager 9.18 上创建了备份，则只能在 Unified Manager 9.18 系统上恢复备份。

- 如果快照配置有任何更改，可能会导致快照无效。

在 Active IQ Unified Manager 中配置 Snapshot 副本位置

您可以使用 ONTAP System Manager 或使用 ONTAP CLI 在您的一个 ONTAP 集群上配置用于存储 Snapshot 副本的卷。

开始之前

集群、存储 VM 和卷必须满足以下要求：

- 集群要求：
  - 必须安装 ONTAP 9.3 或更高版本
  - 它应在地理位置上靠近 Unified Manager 服务器
  - 它可以由 Unified Manager 监控，但不是必需的
- Storage VM 要求：
  - 必须将名称开关和名称映射设置为使用 “files”
  - 为与客户端用户对应而创建的本地用户
  - 确保已选择所有读/写访问权限
  - 确保在导出策略中将超级用户访问权限设置为 “any”

- Linux 版 NetApp Snapshot 的 NFS
- 必须在 NFS 服务器上启用 NFSv4，并在客户端和存储 VM 上指定 NFSv4 ID 域
- 卷大小应至少为 Unified Manager/opt/netapp/data 目录大小的两倍

  使用命令 du -sh /opt/netapp/data/ 检查当前大小。

- 卷要求：
  - 卷大小应至少为 Unified Manager /opt/netapp/data 目录大小的两倍
  - 必须将安全模式设置为 UNIX
  - 必须禁用本地快照策略
  - 应启用卷自动调整大小
  - 应将性能服务级别设置为具有高 IOPS 和低延迟的策略，例如 “Extreme”

有关创建 NFS 卷的详细步骤，请参见 "如何在 ONTAP 9 中配置 NFSv4"和 "ONTAP 9 NFS 配置快速指南"。

在 **Active IQ Unified Manager** 中指定 **Snapshot** 副本的目标位置

您应该在一个 ONTAP 集群中已配置的卷上配置 Active IQ Unified Manager 快照副本的目标位置。您应该使用维护控制台来定义位置。

- 您必须具有安装了 Active IQ Unified Manager 的 Linux 主机的 root 用户凭据。
- 您必须拥有已授权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。
- 您必须具有群集管理 IP 地址、存储 VM 的名称、卷的名称以及存储系统用户名和密码。
- 您必须已将卷装载到 Active IQ Unified Manager 主机，并且必须具有装载路径。

步骤

1. 请使用 Secure Shell 连接到 Active IQ Unified Manager 系统的 IP 地址或 FQDN。
2. 使用维护用户 (umadmin) 名称和密码登录到此系统。
3. 输入命令 `maintenance_console`并按 Enter 键。
4. 在维护控制台*主菜单*中，输入*备份还原*选项的编号。
5. 输入 **Configure NetApp Snapshot Backup** 的编号。
6. 输入要配置 NFS 的编号。
7. 查看您需要提供的信息，然后输入*输入备份配置详细信息*的编号。
8. 要标识要写入快照的卷，请输入集群管理接口的 IP 地址、存储 VM 的名称、卷的名称、LUN 名称、存储系统用户名和密码以及挂载路径。
9. 请验证此信息并输入 `y`。

   系统执行以下任务：

   - 建立与集群的连接
   - 停止所有服务

- 在卷中创建新目录并复制 Active IQ Unified Manager 数据库配置文件
- 从 Active IQ Unified Manager 中删除文件，并创建指向新数据库目录的符号链接
- 重新启动所有服务

10. 请退出维护控制台并启动 Active IQ Unified Manager 界面，以创建快照副本的计划（如果尚未执行此操作）。

在 **Active IQ Unified Manager** 中配置 **Windows** 备份

Active IQ Unified Manager 支持在 Windows 操作系统上借助使用 iSCSI 协议的 LUN，使用 NetApp 快照进行备份和恢复。

可以在所有 Unified Manager 服务运行时进行基于快照的备份。由于备份会对整个数据库施加全局读取锁定以防止任何并发写入，因此作为快照的一部分，将捕获数据库的一致状态。要使 Windows 操作系统上安装的 Unified Manager 系统使用 NetApp 快照执行备份和还原，应首先使用维护控制台将 Unified Manager 备份配置为基于快照的备份。

在配置 Unified Manager 以创建 Snapshot 副本之前，您应执行以下配置任务。

- 配置 ONTAP 集群
- 配置 Windows 主机

在 **Windows** 上配置 **Active IQ Unified Manager** 的备份位置

在 Windows 上备份 Unified Manager 后，应配置用于存储 Snapshot 副本的卷。

开始之前

集群、存储 VM 和卷必须满足以下要求：

- 集群要求：
  - 必须安装 ONTAP 9.3 或更高版本
  - 它应在地理位置上靠近 Unified Manager 服务器
  - 由 Unified Manager 监控
- Storage VM 要求：
  - ONTAP 集群上的 iSCSI 连接
  - 必须为配置的计算机启用 iSCSI 协议
  - 您应该为备份配置提供专用的卷和 LUN。选定的卷应仅包含一个 LUN，不能包含其他任何内容。
  - LUN 的大小应至少是预计在 9.9 Active IQ Unified Manager 中处理的数据大小的两倍。

    这也对卷设置了相同的大小要求。

  - 确保已选择所有读/写访问权限
  - 确保在导出策略中将超级用户访问权限设置为 “any”
- 卷和 LUN 要求：
  - 卷大小应至少为 Unified Manager MySQL 数据目录大小的两倍。

- 必须将安全样式设置为 Windows
- 必须禁用本地快照策略
- 应启用卷自动调整大小
- 应将性能服务级别设置为具有高 IOPS 和低延迟的策略，例如 “Extreme”

在 **Active IQ Unified Manager** 中配置 **ONTAP** 集群以进行备份和还原

在 Windows 系统上使用 Snapshot 副本备份和还原 Active IQ Unified Manager 之前，您需要在 ONTAP 集群上执行一些预配置步骤。

您可以使用命令提示符或 System Manager 用户界面配置 ONTAP 集群。ONTAP 集群的配置包括将数据 LIF 配置为可作为 iSCSI LIF 分配给存储 VM。下一步是使用 System Manager 用户界面配置启用 iSCSI 的存储 VM。您需要为此存储 VM 配置静态网络路由，以控制 LIF 如何使用网络进行出站流量传输。

> 您应该有一个专用卷和一个用于备份配置的 LUN。所选卷应仅包含一个 LUN。LUN 的大小应至少是 Active IQ Unified Manager 预期处理的数据大小的两倍。

您需要执行以下配置：

步骤

1. 配置启用 iSCSI 的存储 VM 或使用具有相同配置的现有存储 VM。
2. 为已配置的 storage VM 配置网络路由。
3. 配置具有适当容量的卷及其内部的单个 LUN，确保该卷仅专用于此 LUN。

> 在 System Manager 上创建 LUN 的情况下，取消 LUN 的映射可能会删除 igroup，并且还原可能会失败。要避免这种情况，请确保在创建 LUN 时，LUN 是显式创建的，并且在取消映射时不会被删除。

4. 在 storage VM 中配置启动程序组。
5. 配置端口集。
6. 将 igroup 与 portset 集成。
7. 将 LUN 映射到 igroup。

在 **Active IQ Unified Manager** 中配置 **Windows** 主机

您需要先配置 Windows 主机，然后才能使用 NetApp 快照备份和还原 Active IQ Unified Manager。要在 Windows 主机上启动 Microsoft iSCSI 启动程序，请在搜索栏中键入 “iscsi” 并单击 **iSCSI Initiator**。

开始之前

您应该清理主机上的所有以前的配置。

如果您尝试在新安装的 Windows 上启动 iSCSI 启动程序，系统会提示您进行确认，确认后，将显示 iSCSI 属性对话框。如果是现有的 Windows 安装，则会显示 iSCSI 属性对话框，其中的目标处于非活动状态或正在尝试连接。因此，您需要确保删除 Windows 主机上所有以前的配置。

步骤

1. 清理主机上的所有先前配置。
2. 发现目标门户。
3. 连接到目标门户。
4. 使用多路径连接到目标门户。
5. 发现这两个 LIF。
6. 发现 Windows 计算机中配置为设备的 LUN。
7. 在 Windows 中将发现的 LUN 配置为新的卷驱动器。

在 **Active IQ Unified Manager** 中指定 **Windows** 上 **Snapshot** 副本的目标位置

您应该在一个 ONTAP 集群中已配置的卷上配置 Active IQ Unified Manager 快照副本的目标位置。您应该使用维护控制台来定义位置。

- 您必须拥有安装了 Active IQ Unified Manager 的 Windows 主机的管理员权限。
- 您必须拥有已授权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。
- 必须具有群集管理 IP 地址、存储 VM 的名称、卷的名称、LUN 名称以及存储系统用户名和密码。
- 您必须已将卷作为网络驱动器装载到 Active IQ Unified Manager 主机，并且必须具有装载驱动器。

步骤

1. 请使用 Power Shell 连接到 Active IQ Unified Manager 系统的 IP 地址或完全限定域名。
2. 使用维护用户 (umadmin) 名称和密码登录到此系统。
3. 输入命令 `maintenance_console`并按 Enter 键。
4. 在维护控制台*主菜单*中，输入*备份还原*选项的编号。
5. 输入 **Configure NetApp Snapshot Backup** 的编号。
6. 输入编号以配置 iSCSI。
7. 查看您需要提供的信息，然后输入*输入备份配置详细信息*的编号。
8. 要标识将写入快照的卷，请输入集群管理接口的 IP 地址、存储 VM 的名称、卷的名称、LUN 名称、存储系统用户名和密码以及挂载驱动器。
9. 请验证此信息并输入 `y`。

   系统执行以下任务：

   - Storage VM 已验证
   - 卷已验证
   - 挂载驱动器和状态已验证
   - LUN 存在性和状态
   - 网络驱动器存在
   - 已验证挂载卷上存在推荐空间（超过 mysql 数据目录的两倍）
   - 与卷中的专用 LUN 对应的 LUN 路径

- igroup 名称
- 装载网络驱动器的卷的 GUID
- 用于与 ONTAP 通信的 iSCSI 启动程序

10. 退出维护控制台并启动 Active IQ Unified Manager 界面以创建快照副本计划。

在 **Active IQ Unified Manager** 的维护控制台中配置 **Snapshot** 备份

要使用 Snapshot 副本进行 Active IQ Unified Manager 备份，应从维护控制台执行一些配置步骤。

开始之前

您应具备系统的以下详细信息：

- 集群 IP 地址
- Storage VM 名称
- Volume name
- LUN 名称
- 挂载路径
- 存储系统凭据

步骤

1. 访问 Unified Manager 的维护控制台。
2. 输入 4 以选择*备份还原*。
3. 输入 2 以选择 使用 **NetApp** 快照备份和还原。

> 如果要更改备份配置，请输入 3 以选择 更新 **NetApp Snapshot** 备份配置。您只能更新密码。

4. 从菜单中，输入 1 以选择 配置 **NetApp Snapshot** 备份。
5. 输入 1 以提供所需的信息。
6. 提供维护控制台的用户名和密码，然后确认 LUN 已挂载到主机上。

   然后，该过程会验证您提供的数据目录、LUN 路径、存储 VM、卷、空间可用性、驱动器等是否正确。在后台进行的操作包括：

   - 服务已停止
   - 数据库目录已移动到已挂载的存储
   - 数据库目录已删除，符号链接已建立
   - 服务重新启动。在 Active IQ Unified Manager 界面中完成配置后，备份类型将修改为 NetApp Snapshot ，并在用户界面中显示为数据库备份（基于 Snapshot）。

在开始备份操作之前，必须检查 Snapshot 配置中是否存在任何更改，因为这可能会导致快照无效。假设您在 G 驱动器中配置了备份，并创建了 Snapshot。您后来将备份重新配置为 E 驱动器，并根据新配置将数据保存到 E

驱动器。如果您尝试恢复在 G 驱动器中创建的 Snapshot，它将失败，并显示错误 G 驱动器不存在。

在 **Active IQ Unified Manager** 中定义 **Linux** 和 **Windows** 的备份计划

您可以使用 Unified Manager UI 配置创建 Unified Manager Snapshot 副本的计划。

开始之前

- 您必须具有操作员、应用程序管理员或存储管理员角色。
- 您必须已配置从维护控制台创建 Snapshot 副本的设置，以确定将创建快照的目标。

Snapshot 副本仅需几分钟即可创建，而 Unified Manager 数据库仅锁定几秒钟。

在新集群添加的最初 15 天内进行的备份可能不够准确，无法获取历史性能数据。

步骤

1. 在左侧导航窗格中，单击 常规 > 数据库备份。
2. 在*数据库备份*页面中，单击*备份设置*。
3. 在*保留计数*字段中输入要保留的最大 Snapshot 副本数。

   保留计数的默认值为 10。Snapshot 副本的最大数量由集群上的 ONTAP 软件版本决定。您可以将此字段留空以实现最大值，无论 ONTAP 版本如何。
4. 选择*每日计划*或*每周计划*按钮，然后指定计划详细信息。
5. 单击*应用*。

Snapshot 副本是根据计划创建的。您可以在“数据库备份”页面中查看可用的备份文件。

由于此卷和快照的重要性，您可能需要为此卷创建一个或两个警报，以便在以下任一情况下通知您：

- 卷空间已满 90%。使用事件*卷空间已满*设置警报。

  您可以使用 ONTAP System Manager 或 ONTAP CLI 向卷添加容量，以便 Unified Manager 数据库不会用尽空间。
- 快照数量接近最大数量。使用事件 **Too Many Snapshot Copies** 设置警报。

  您可以使用 ONTAP System Manager 或 ONTAP CLI 删除较旧的快照，以便始终为新的 Snapshot 副本留出空间。

您可以在“警报设置”页面中配置警报。

使用 **Snapshot** 副本还原 **Active IQ Unified Manager**

如果发生数据丢失或数据损坏，您可以将 Unified Manager 恢复到以前的稳定状态，并将数据丢失降到最低。您可以使用 Unified Manager 维护控制台将 Unified Manager 快照数据库还原到本地或远程操作系统。

开始之前

- 您必须具有 Linux 主机的 root 用户凭据和安装了 Unified Manager 的 Windows 主机的管理权限。
- 您必须拥有已授权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。

还原功能是特定于平台和版本的。您只能在相同版本的 Unified Manager 上还原 Unified Manager 备份。

步骤

1. 连接到 Unified Manager 系统的 IP 地址或完全限定的域名。
   - Linux：安全 Shell
   - Windows：Power Shell
2. 使用 root 用户凭据登录到系统。
3. 输入命令 `maintenance_console`并按 Enter 键。
4. 在维护控制台*主菜单*中，为*备份还原*选项输入 4。
5. 输入 2 以选择*使用 NetApp 快照备份和还原*。

   如果要对新服务器执行还原，安装 Unified Manager 后，请不要启动 UI，也不要在安装完成后配置任何集群、用户或身份验证设置。输入 1 以选择 配置 **NetApp Snapshot** 备份，并按照原始系统上的设置配置 Snapshot 副本。
6. 输入 3 以选择*使用 NetApp 快照还原*。
7. 选择要从中还原 Unified Manager 的快照副本。按 **Enter** 键。
8. 还原过程完成后，登录到 Unified Manager 用户界面。

恢复备份后，如果 Workflow Automation 服务器无法正常工作，请执行以下步骤：

1. 在 Workflow Automation 服务器上，更改 Unified Manager 服务器的 IP 地址以指向最新的计算机。
2. 如果在步骤 1 中采集失败，请在 Unified Manager 服务器上重置数据库密码。

在 **Active IQ Unified Manager** 中修改备份类型

如果要更改 Active IQ Unified Manager 系统的备份类型，则可以使用维护控制台选项。*取消配置 NetApp 快照备份*选项使您可以回退到基于 MySQL 的备份。

开始之前

您必须拥有已授权登录到 Unified Manager 服务器维护控制台的用户 ID 和密码。

步骤

1. 访问维护控制台。
2. 从*主菜单*中选择 4 进行备份和还原。
3. 从 备份和还原菜单 中选择 2。
4. 为*取消配置 NetApp 快照备份*选择 4。

   将显示执行的操作，即停止服务、中断符号链接、将数据从存储移动到目录，然后重新启动服务。

   修改备份方法后，备份机制从 Snapshot copy 更改为默认 MySQL 备份。此更改将显示在常规设置的“数据

库备份”部分。

了解 **Active IQ Unified Manager** 的按需备份

您可以在需要时使用 Active IQ Unified Manager 用户界面生成按需备份。通过按需备份，您可以使用现有备份方法即时创建备份。按需备份不会区分 MySQL 或基于 NetApp 快照的备份。

您可以使用数据库备份页面上的*立即备份*按钮执行按需备份。按需备份不依赖于您为 Active IQ Unified Manager 配置的计划。

将 **Active IQ Unified Manager** 虚拟设备迁移到 **Linux** 系统

如果要更改运行 Unified Manager 的主机操作系统，则可以将 Unified Manager MySQL 数据库转储备份从虚拟设备恢复到 Red Hat Enterprise Linux 系统。

开始之前

- 在虚拟设备上：
  - 您必须具有操作员、应用程序管理员或存储管理员角色。
  - 您必须知道还原操作的 Unified Manager 维护用户的名称。
- 在 Linux 系统上：
  - 您必须已按照 "在 Linux 系统上安装 Unified Manager" 中的说明在 Linux 服务器上安装 Unified Manager。
  - 此服务器上的 Unified Manager 版本必须与使用备份文件的虚拟设备上的版本相同。
  - 安装后，请勿在 Linux 系统上启动 UI 或配置任何集群、用户或身份验证设置。在还原过程中，备份文件会填充此信息。
  - 您必须具有 Linux 主机的 root 用户凭据。

这些步骤介绍了如何在虚拟设备上创建备份文件，将备份文件复制到 Red Hat Enterprise Linux，然后将数据库备份还原到新系统。

步骤

1. 在虚拟设备上，单击*管理* > 数据库备份。
2. 在*数据库备份*页面中，单击*备份设置*。
3. 将备份路径更改为 /jail/support。
4. 在计划部分，选择*每日计划*，然后输入比当前时间晚几分钟的时间，以便很快创建备份。
5. 单击*应用*。
6. 请等待几个小时，以便生成备份。

   完整备份可能超过 1 GB，可能需要三到四个小时才能完成。

7. 以 root 用户身份登录到安装了 Unified Manager 的 Linux 主机，并使用 SCP 从虚拟设备上的 /support 复制备份文件.`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/*`
   .

```
root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
```

确保已复制 /database-dumps-repo 子目录中的 .7z 备份文件和所有 .7z 存储库文件。

8. 在命令提示符处，还原备份： `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. 恢复操作完成后，登录到 Unified Manager Web UI。

您应执行以下任务：

- 生成新的 HTTPS 安全证书并重新启动 Unified Manager 服务器。
- 将备份路径更改为 Linux 系统的默认设置（/data/ocum-backup），或更改为您选择的新路径，因为 Linux 系统上没有 /jail/support 路径。
- 如果正在使用 WFA，请重新配置 Workflow Automation 连接的两端。
- 如果您使用的是 SAML，请重新配置 SAML 身份验证设置。

验证 Linux 系统上的所有内容均按预期运行后，您可以关闭并删除 Unified Manager 虚拟设备。

管理脚本

在 **Active IQ Unified Manager** 中管理脚本

您可以使用脚本自动修改或更新 Unified Manager 中的多个存储对象。该脚本与警报相关联。当事件触发警报时，将执行脚本。您可以在生成警报时上传自定义脚本并测试其执行情况。

默认情况下，将脚本上传到 Unified Manager 并运行它们的功能处于启用状态。如果您的组织出于安全原因不想允许此功能，您可以从*存储管理* > *功能设置*禁用此功能。

了解脚本如何与 **Active IQ Unified Manager** 中的警报配合使用

您可以将警报与脚本关联，以便在 Unified Manager 中引发事件警报时执行脚本。您可以使用脚本来解决存储对象的问题或识别哪些存储对象正在生成事件。

在 Unified Manager 中为事件生成警报时，将向指定收件人发送警报电子邮件。如果您将警报与脚本相关联，则会执行脚本。您可以从警报电子邮件中获取传递给脚本的参数的详细信息。

如果您已创建自定义脚本并将其与特定事件类型的警报相关联，则将根据该事件类型的自定义脚本采取操作，默认情况下，“管理操作”页面或 Unified Manager 仪表板上的“修复它”操作不可用。

该脚本使用以下参数执行：

- `-eventID`
- `-eventName`

- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

您可以在脚本中使用参数并收集相关事件信息或修改存储对象。

从脚本中获取参数的示例

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

生成警报时，系统将执行此脚本并显示以下输出：

```
-eventID : 290
-eventSourceID : 4138
```

在 **Active IQ Unified Manager** 中添加脚本

您可以在 Unified Manager 中添加脚本，并将脚本与警报相关联。这些脚本在生成警报时自动执行，使您能够获得有关为其生成事件的存储对象的信息。

开始之前

- 必须已创建并保存要添加到 Unified Manager 服务器的脚本。
- 支持的脚本文件格式有 Perl、Shell、PowerShell、Python 和 `.bat` 文件。

安装 **Unified Manager** 的平台	支持的语言
VMware	Perl 和 Shell 脚本
Linux	Perl、Python 和 Shell 脚本
Windows	PowerShell、Perl、Python 和 .bat 脚本

  - 对于 Perl 脚本，必须在 Unified Manager 服务器上安装 Perl。对于 VMware 安装，默认情况下会安装 Perl 5，脚本将仅支持 Perl 5 支持的内容。如果 Perl 是在 Unified Manager 之后安装的，则必须重新启动 Unified Manager 服务器。
  - 对于 PowerShell 脚本，必须在 Windows 服务器上设置相应的 PowerShell 执行策略，以便能够执行这些脚本。

> 如果您的脚本创建日志文件以跟踪警报脚本进度，则必须确保不会在 Unified Manager 安装文件夹中的任何位置创建日志文件。

- 您必须具有应用程序管理员或存储管理员角色。

您可以上传自定义脚本，并收集有关警报的事件详细信息。

> 如果在用户界面中看不到此功能，则是因为管理员已禁用此功能。如果需要，您可以从*存储管理* > *功能设置*启用此功能。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 脚本。
2. 在*脚本*页面中，单击*添加*。
3. 在*添加脚本*对话框中，单击*浏览*以选择您的脚本文件。
4. 输入选定脚本的说明。
5. 单击 **Add**。

删除 **Active IQ Unified Manager** 中的脚本

当脚本不再需要或有效时，您可以从 Unified Manager 中删除该脚本。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 此脚本不得与警报相关联。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 脚本。
2. 在*脚本*页面中，选择要删除的脚本，然后单击*删除*。
3. 在*警告*对话框中，单击*是*确认删除。

在 **Active IQ Unified Manager** 中执行测试脚本

您可以验证在针对存储对象生成警报后是否正确执行了您的脚本。

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已将支持的文件格式的脚本上载到 Unified Manager。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 脚本。
2. 在“脚本”页面中，添加测试脚本。
3. 在左侧导航窗格中，单击*存储管理* > 警报设置。
4. 在*警报设置*页面中，执行以下操作之一：

目的	操作
添加警报	a. 单击 **Add**。 b. 在操作部分，将警报与测试脚本相关联。

目的	操作
编辑警报	a. 选择一个警报，然后单击*编辑*。 b. 在操作部分，将警报与测试脚本相关联。

5. 单击 **Save**。
6. 在*警报设置*页面中，选择您添加或修改的警报，然后单击*测试*。

   使用“`-test`”参数执行脚本，并向创建警报时指定的电子邮件地址发送通知警报。

管理和监控组

了解组

了解 **Active IQ Unified Manager** 中的组

组是异构存储对象（集群、SVM 或卷）的动态集合。您可以在 Unified Manager 中创建组，以轻松管理一组存储对象。组中的成员可能会发生变化，具体取决于 Unified Manager 在某个时间点监控的存储对象。

- 每个组都有一个唯一的名称。
- 您必须为每个组配置至少一个组规则。
- 您可以将组与多个组规则关联。
- 每个组可以包括多种类型的存储对象，例如集群、SVM 或卷。
- 存储对象将根据组规则的创建时间或 Unified Manager 完成监控周期的时间动态添加到组中。
- 您可以同时对组中的所有存储对象应用操作，例如为卷设置阈值。

了解 **Active IQ Unified Manager** 中组的组规则工作方式

组规则是您为使存储对象（卷、群集或 SVM）包含在特定组中而定义的标准。您可以使用条件组或条件来定义组的组规则。

- 您必须将组规则关联到组。
- 您必须为组规则关联对象类型；只有一个对象类型与组规则关联。
- 在每个监控周期之后，或者在创建、编辑或删除规则时，存储对象将被添加到组中或从组中移除。
- 组规则可以有一个或多个条件组，每个条件组可以有一个或多个条件。
- 存储对象可以根据您创建的组规则属于多个组。

条件

您可以创建多个条件组，每个条件组可以有一个或多个条件。您可以将组规则中定义的所有条件组应用于组，以指定组中包括哪些存储对象。

条件组中的条件使用逻辑 AND 执行。必须满足条件组中的所有条件。创建或修改组规则时，将创建一个条件，该条件仅适用、选择和分组满足条件组中所有条件的存储对象。如果要缩小要在组中包含哪些存储对象的范围，

则可以在条件组中使用多个条件。

您可以使用以下操作数和运算符并指定所需的值，使用存储对象创建条件。

存储对象类型	适用的操作数
卷	• 对象名称 • 所属集群名称 • 所属 SVM 名称 • 标注
SVM	• 对象名称 • 所属集群名称 • 标注
集群	• 对象名称 • 标注

当您选择批注作为任何存储对象的操作数时，“Is”运算符可用。对于所有其他操作数，您可以选择“Is”或“Contains”作为运算符。

- 操作数

  Unified Manager 中的操作数列表会根据选定对象类型进行更改。该列表包括对象名称、拥有群集名称、拥有 SVM 名称以及您在 Unified Manager 中定义的注释。

- 运算符

  运算符列表会根据为条件选择的操作数而变化。Unified Manager 支持的运算符为 “Is” 和 “Contains”。

  当您选择“Is”运算符时，将对该条件进行评估，以确保操作数值与为选定操作数提供的值完全匹配。

  当您选择“包含”运算符时，条件将被评估为满足以下条件之一：

  - 操作数值与为选定操作数提供的值完全匹配
  - 操作数值包含为选定操作数提供的值

- 值

  值字段将根据所选操作数进行更改。

带条件的组规则示例

考虑具有以下两个条件的卷的条件组：

- 名称包含 “vol”
- SVM 名称为 “data_svm”

此条件组选择所有在其名称中包含“vol”且托管在名为“data_svm”的 SVM 上的卷。

条件组

条件组使用逻辑 OR 执行，然后应用于存储对象。存储对象必须满足其中一个条件组才能包含在组中。所有条件组的存储对象将组合在一起。您可以使用条件组来扩大要包含在组中的存储对象的范围。

带条件组的组规则示例

考虑一个卷的两个条件组，每个组包含以下两个条件：

- 条件组 1
  - 名称包含 “vol”
  - SVM 名称为“data_svm”条件组 1 选择名称中包含“vol”且托管在名为“data_svm”的 SVM 上的所有卷。
- 条件组 2
  - 名称包含 “vol”
  - 数据优先级的批注值为 “critical” 条件组 2 选择名称中包含 “vol” 且使用数据优先级批注值标注为 “critical” 的所有卷。

如果对存储对象应用包含这两个条件组的组规则，则会将以下存储对象添加到所选组：

- 所有在名称中包含“vol”且托管在名为“data_svm”的 SVM 上的卷。
- 所有在其名称中包含“vol”且使用数据优先级标注值“critical”进行标注的卷。

了解组操作如何在 **Active IQ Unified Manager** 中的存储对象上运行

组操作是对组中的所有存储对象执行的操作。例如，您可以配置卷阈值组操作来同时更改组中所有卷的卷阈值。

组支持唯一的组操作类型。一个组只能有一种卷运行状况阈值组操作类型。但是，您可以为同一组配置不同类型的组操作（如果可用）。组操作的等级决定了操作应用于存储对象的顺序。存储对象的详细信息页面提供了有关对存储对象应用了哪种组操作的信息。

唯一组操作示例

假设卷 A 属于组 G1 和 G2，并且为这些组配置了以下卷健康阈值组操作：

- Change_capacity_threshold group action with rank 1，用于配置卷的容量
- Change_snapshot_copies 级别为 2 的 group 操作，用于配置卷的 Snapshot 副本

> `Change_capacity_threshold`组操作始终优先于`Change_snapshot_copies`组操作并应用于卷 A。当 Unified Manager 完成一个监控周期时，将根据 `Change_capacity_threshold`组操作重新评估卷 A 的健康阈值相关事件。您不能为 G1 或 G2 组配置其他卷阈值类型的组操作。

在 **Active IQ Unified Manager** 中添加组

可以创建组来组合集群、卷和存储虚拟机（SVM），以便于管理。

开始之前

您必须具有应用程序管理员或存储管理员角色。

您可以定义组规则以从组中添加或删除成员，并修改组的组操作。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。
2. 在*群组*选项卡中，单击*添加*。
3. 在*添加组*对话框中，输入组的名称和描述。
4. 单击 **Add**。

在 **Active IQ Unified Manager** 中编辑组

您可以编辑在 Unified Manager 中创建的组的名称和描述。

开始之前

您必须具有应用程序管理员或存储管理员角色。

编辑组以更新名称时，必须指定唯一的名称；不能使用现有的组名称。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。
2. 在*组*选项卡中，选择要编辑的组，然后单击*编辑*。
3. 在*编辑组*对话框中，更改组的名称、描述或两者。
4. 单击 **Save**。

删除 **Active IQ Unified Manager** 中的组

当组不再需要时，您可以从 Unified Manager 中删除该组。

开始之前

- 任何存储对象（群集、SVM 或卷）都不得与同您要删除的组相关联的任何组规则相关联。
- 您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。
2. 在*组*选项卡中，选择要删除的组，然后单击*删除*。
3. 在*警告*对话框中，单击*是*确认删除。

   删除组不会删除与该组相关联的组操作。但是，在删除组后，这些组操作将被取消映射。

在 **Active IQ Unified Manager** 中添加组规则

您可以为组创建组规则，以便将卷、集群或 Storage Virtual Machine （SVM） 等存储对象动态添加到组中。您必须配置至少包含一个条件的一个条件组，才能创建组规则。

开始之前

您必须具有应用程序管理员或存储管理员角色。

创建组规则后，将立即添加当前受监控的存储对象。只有在监控周期完成后才会添加新对象。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。
2. 在*组规则*选项卡中，单击*添加*。
3. 在*添加组规则*对话框中，指定组规则的名称。
4. 在*目标对象类型*字段中，选择要分组的存储对象类型。
5. 在*组*字段中，选择要为其创建组规则的所需组。
6. 在*条件*部分中，执行以下步骤来创建条件、条件组或两者：

要创建.....	操作
一个条件	a. 从操作数列表中选择操作数。 b. 选择*包含*或*是*作为运算符。 c. 请输入一个值，或从可用列表中选择一个值。
条件组	a. 单击 添加条件组 b. 从操作数列表中选择操作数。 c. 选择*包含*或*是*作为运算符。 d. 请输入一个值，或从可用列表中选择一个值。 e. 如果需要，单击*添加条件*以创建更多条件，然后对每个条件重复步骤 a 至 d。

7. 单击 **Add**。

创建组规则示例

在“添加组规则”对话框中执行以下步骤以创建组规则，包括配置条件和添加条件组：

步骤

1. 指定组规则的名称。
2. 选择对象类型为 Storage Virtual Machine (SVM)。
3. 从组列表中选择一个组。
4. 在条件部分，选择*对象名称*作为操作数。
5. 选择*包含*作为运算符。

6. 输入值为 `svm_data`。
7. 单击*添加条件组*。
8. 选择*对象名称*作为操作数。
9. 选择*包含*作为运算符。
10. 将值输入为 `vol`。
11. 单击*添加条件*。
12. 重复步骤 8 至 10，在步骤 8 中选择 **data-priority** 作为操作数，在步骤 9 中选择 **Is** 作为运算符，在步骤 10 中选择 **critical** 作为值。
13. 单击 添加 以创建组规则的条件。

在 **Active IQ Unified Manager** 中编辑组规则

您可以编辑组规则以修改条件组以及条件组中的条件，以便在特定组中添加或删除存储对象。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。
2. 在*组规则*选项卡中，选择要编辑的组规则，然后单击*编辑*。
3. 在*编辑组规则*对话框中，根据需要更改组规则名称、关联的组名称、条件组和条件。

   无法更改组规则的目标对象类型。

4. 单击 **Save**。

删除 **Active IQ Unified Manager** 中的组规则

当不再需要组规则时，您可以从 Active IQ Unified Manager 中删除组规则。

开始之前

您必须具有应用程序管理员或存储管理员角色。

删除组规则时，关联的存储对象将从组中删除。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。
2. 在*组规则*选项卡中，选择要删除的组规则，然后单击*删除*。
3. 在*警告*对话框中，单击*是*确认删除。

在 **Active IQ Unified Manager** 中添加组操作

您可以配置要应用于组中存储对象的组操作。为组配置操作可以节省时间，因为您不必将这些操作单独添加到每个对象。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。
2. 在*组操作*选项卡中，单击*添加*。
3. 在*添加组操作*对话框中，输入操作的名称和描述。
4. 从*组*菜单中，选择要为其配置操作的组。
5. 在*操作类型*菜单中，选择一种操作类型。

   对话框展开，使您可以使用所需的参数配置所选操作类型。
6. 为配置组操作所需的参数输入适当的值。
7. 单击 **Add**。

在 **Active IQ Unified Manager** 中编辑组操作

您可以编辑在 Unified Manager 中配置的组操作参数，例如组操作名称、说明、关联的组名称以及操作类型的参数。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。
2. 在*组操作*选项卡中，选择要编辑的组操作，然后单击*编辑*。
3. 在*编辑组操作*对话框中，根据需要更改组操作名称、描述、关联的组名称和操作类型的参数。
4. 单击 **Save**。

在 **Active IQ Unified Manager** 中为组配置卷运行状况阈值

您可以为容量、Snapshot 副本、qtree 配额、增长和 inode 配置组级卷运行状况阈值。

开始之前

您必须具有应用程序管理员或存储管理员角色。

组操作的卷运行状况阈值类型仅应用于组的卷。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。

2. 在*组操作*选项卡中，单击*添加*。
3. 输入组操作的名称和描述。
4. 从*组*下拉框中，选择要为其配置组操作的组。
5. 选择*操作类型*作为卷运行状况阈值。
6. 选择要设置阈值的类别。
7. 输入运行状况阈值的所需值。
8. 单击 **Add**。

删除 **Active IQ Unified Manager** 中的组操作

当不再需要组操作时，您可以从 Unified Manager 中删除组操作。

开始之前

您必须具有应用程序管理员或存储管理员角色。

当您删除卷运行状况阈值的组操作时，全局阈值将应用于该组中的存储对象。存储对象上设置的任何对象级运行状况阈值都不会受到影响。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。
2. 在*组操作*选项卡中，选择要删除的组操作，然后单击*删除*。
3. 在*警告*对话框中，单击*是*确认删除。

在 **Active IQ Unified Manager** 中重新排序组操作

您可以更改要应用于组中存储对象的组操作的顺序。组操作会根据其等级顺序应用于存储对象。最低等级将分配给您最后配置的组操作。您可以根据要求更改组操作的等级。

开始之前

您必须具有应用程序管理员或存储管理员角色。

您可以选择单行或多行，然后执行多个拖放操作以更改组操作的排名。但是，您必须保存更改，以便在组操作网格中反映重新排序的优先级。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 组。
2. 在*组操作*选项卡中，单击*重新排序*。
3. 在*重新排序组操作*对话框中，拖放行以根据需要重新排列组操作的顺序。
4. 单击 **Save**。

使用注释确定存储对象事件的优先级

详细了解注释

了解 **Active IQ Unified Manager** 中的注释

注释是分配给另一个文本字符串（值）的文本字符串（名称）。每个注释名称-值对可以使用注释规则与存储对象动态关联。将存储对象与预定义的注释相关联时，您可以筛选和查看与其相关的事件。您可以将注释应用于集群、卷和存储虚拟机（SVM）。

每个批注名称可以有多个值；每个名称-值对可以通过规则与存储对象相关联。

例如，您可以使用值“Boston”和“Canada”创建名为“data-center”的批注。然后，您可以将值为“Boston”的批注“data-center”应用于卷 v1。当为带有“data-center”批注的卷 v1 上的任何事件生成警报时，生成的电子邮件会指示卷的位置“Boston”，这使您能够确定问题的优先级并解决问题。

了解注释规则在 **Active IQ Unified Manager** 中的工作原理

标注规则是您定义的用于标注存储对象（卷、集群或存储虚拟机 (SVM)）的标准。您可以使用条件组或条件来定义标注规则。

- 必须将批注规则与批注相关联。
- 必须为批注规则关联对象类型；只能为批注规则关联一个对象类型。
- Unified Manager 在每个监控周期之后，或者在创建、编辑、删除或重新排序规则时，为存储对象添加或删除注释。
- 注释规则可以有一个或多个条件组，每个条件组可以有一个或多个条件。
- 存储对象可以有多个注释。特定注释的注释规则还可以在规则条件中使用不同的注释，以向已注释的对象添加另一个注释。

条件

您可以创建多个条件组，每个条件组可以有一个或多个条件。可以在批注的批注规则中应用所有定义的条件组，以便对存储对象进行批注。

条件组中的条件使用逻辑 AND 执行。必须满足条件组中的所有条件。创建或修改批注规则时，将创建一个条件，该条件仅适用、选择和批注满足条件组中所有条件的存储对象。如果要缩小要批注的存储对象的范围，可以在一个条件组中使用多个条件。

您可以使用以下操作数和运算符并指定所需的值，使用存储对象创建条件。

存储对象类型	适用的操作数
卷	• 对象名称 • 所属集群名称 • 所属 SVM 名称 • 标注

存储对象类型	适用的操作数
SVM	• 对象名称 • 所属集群名称 • 标注
集群	• 对象名称 • 标注

当您选择批注作为任何存储对象的操作数时，“Is”运算符可用。对于所有其他操作数，您可以选择“Is”或“Contains”作为运算符。当您选择“Is”运算符时，将对条件进行求值，以确保操作数值与为所选操作数提供的值完全匹配。当您选择“Contains”运算符时，条件将被评估为满足以下条件之一：

- 操作数值与选定操作数值完全匹配。
- 操作数值包含为选定操作数提供的值。

带条件的批注规则示例

考虑针对卷的具有一个条件组的注释规则，其中包含以下两个条件：

- 名称包含 “vol”
- SVM 名称为 “data_svm”

此注释规则使用所选注释和注释类型注释所有在名称中包含“vol”且托管在名为“data_svm”的 SVM 上的卷。

条件组

条件组使用逻辑 OR 执行，然后应用于存储对象。存储对象必须满足其中一个条件组的要求才能进行标注。满足所有条件组条件的存储对象将被标注。您可以使用条件组来扩大要标注的存储对象的范围。

带条件组的批注规则示例

考虑针对一个卷具有两个条件组的批注规则；每个组包含以下两个条件：

- 条件组 1
  - 名称包含 “vol”
  - SVM 名称为 “data_svm” 此条件组注释名称中包含 “vol” 且托管在名为 “data_svm” 的 SVM 上的所有卷。
- 条件组 2
  - 名称包含 “vol”
  - 数据优先级的批注值为“critical”。此条件组将批注所有名称中包含“vol”且数据优先级批注值为“critical”的卷。

当对存储对象应用包含这两个条件组的批注规则时，将对以下存储对象进行批注：

- 所有在名称中包含 “vol” 且托管在名为 “data_svm” 的 SVM 上的卷。
- 所有在名称中包含 “vol” 且使用数据优先级标注值标注为 “critical” 的卷。

了解 **Active IQ Unified Manager** 中的预定义注释值

数据优先级 是一种预定义批注，其值为关键任务、高和低。这些值使您能够根据存储对象包含的数据的优先级对其进行批注。您无法编辑或删除预定义的批注值。

- 数据优先级：关键任务

  此注释适用于包含关键任务数据的存储对象。例如，包含生产应用程序的对象可被视为关键任务。

- 数据优先级：高

  此批注应用于包含高优先级数据的存储对象。例如，托管业务应用程序的对象可以被视为高优先级。

- 数据优先级：低

  此批注应用于包含低优先级数据的存储对象。例如，位于辅助存储上的对象（如备份和镜像目标）的优先级可能较低。

在 **Active IQ Unified Manager** 中动态添加注释

创建自定义注释时，Unified Manager 会使用规则将集群、存储虚拟机（SVM）和卷与注释动态关联。这些规则会自动将注释分配给存储对象。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 存储管理 > 注释。
2. 在*注释*页面中，单击*添加注释*。
3. 在*添加注释*对话框中，键入注释的名称和描述。
4. 可选：在*注释值*部分，单击*添加*以向注释添加值。
5. 单击 **Save**。

在 **Active IQ Unified Manager** 中向注释添加值

您可以向批注添加值，然后将存储对象与特定的批注名称-值对关联起来。向批注添加值可帮助您更有效地管理存储对象。

开始之前

您必须具有应用程序管理员或存储管理员角色。

您不能将值添加到预定义的注释。

步骤

1. 在左侧导航窗格中，单击 存储管理 > 注释。
2. 在*注释*页面中，选择要向其添加值的注释，然后在*值*部分中单击*添加*。
3. 在*添加批注值*对话框中，指定批注值。

指定的值对于选定的标注必须是唯一的。

4. 单击 **Add**。

删除 **Active IQ Unified Manager** 中的注释

当不再需要自定义注释及其值时，您可以将其删除。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 不得在其他注释或组规则中使用注释值。

步骤

1. 在左侧导航窗格中，单击 存储管理 > 注释。
2. 在*注释*选项卡中，选择要删除的注释。

   将显示所选批注的详细信息。

3. 单击*操作* > *删除*以删除选定注释及其值。
4. 在警告对话框中，单击*是*确认删除。

在 **Active IQ Unified Manager** 中查看注释列表和详细信息

您可以查看与集群、卷和存储虚拟机（SVM）动态关联的批注列表。您还可以查看详细信息，例如描述、创建者、创建日期、值、规则以及与批注关联的对象。

步骤

1. 在左侧导航窗格中，单击 存储管理 > 注释。
2. 在*注释*选项卡中，单击注释名称以查看相关详细信息。

从 **Active IQ Unified Manager** 中删除注释中的值

当与自定义批注关联的值不再应用于批注时，您可以删除该值。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 标注值不得与任何标注规则或组规则关联。

您不能从预定义的注释中删除值。

步骤

1. 在左侧导航窗格中，单击 存储管理 > 注释。
2. 在*批注*选项卡的批注列表中，选择要从中删除值的批注。
3. 在*注释*选项卡的*值*区域中，选择要删除的值，然后单击*删除*。
4. 在*警告*对话框中，单击*是*。

该值将被删除，不再显示在所选标注的值列表中。

在 **Active IQ Unified Manager** 中创建标注规则

您可以创建批注规则， Unified Manager 使用这些规则动态批注卷、集群或 Storage Virtual Machine （SVM） 等存储对象。

开始之前

您必须具有应用程序管理员或存储管理员角色。

创建注释规则后，将立即对当前受监控的存储对象进行注释。只有在监控周期完成后，才会对新对象进行注释。

步骤

1. 在左侧导航窗格中，单击 存储管理 > 注释。
2. 在*注释规则*选项卡中，单击*添加*。
3. 在*添加注释规则*对话框中，为注释规则指定一个名称。
4. 在*目标对象类型*字段中，选择要注释的存储对象类型。
5. 在*应用注释*字段中，选择要使用的注释和注释值。
6. 在条件部分中，执行相应的操作以创建条件、条件组或两者：

要创建.....	操作
一个条件	a. 从操作数列表中选择操作数。 b. 选择*包含*或*是*作为运算符。 c. 请输入一个值，或从可用列表中选择一个值。
条件组	a. 单击*添加条件组*。 b. 从操作数列表中选择操作数。 c. 选择*包含*或*是*作为运算符。 d. 请输入一个值，或从可用列表中选择一个值。 e. 如果需要，单击*添加条件*以创建更多条件，然后对每个条件重复步骤 a 至 d。

7. 单击 **Add**。

创建批注规则的示例

在“添加批注规则”对话框中执行以下步骤以创建批注规则，包括配置条件和添加条件组：

步骤

1. 指定批注规则的名称。
2. 选择目标对象类型为 Storage Virtual Machine (SVM)。
3. 从批注列表中选择一个批注，并指定一个值。
4. 在条件部分，选择*对象名称*作为操作数。

5. 选择*包含*作为运算符。
6. 输入值为 `svm_data`。
7. 单击*添加条件组*。
8. 选择*对象名称*作为操作数。
9. 选择*包含*作为运算符。
10. 将值输入为 `vol`。
11. 单击*添加条件*。
12. 重复步骤 8 至 10，在步骤 8 中选择 **data-priority** 作为操作数，在步骤 9 中选择 **Is** 作为运算符，在步骤 10 中选择 **mission-critical** 作为值。
13. 单击 **Add**。

在 **Active IQ Unified Manager** 中手动向单个存储对象添加注释

您可以手动标注选定的卷、集群和 SVM，而无需使用标注规则。您可以标注单个存储对象或多个存储对象，并为标注指定所需的名称-值对组合。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 导航到要注释的存储对象：

要将注释添加到……	操作
集群	a. 单击 **Storage** > **Clusters**。 b. 选择一个或多个群集。
卷	a. 单击 **Storage** （存储） > **Volumes** （卷）。 b. 选择一个或多个卷。
SVM	a. 单击 存储 > **SVMs**。 b. 选择一个或多个 SVM。

2. 单击*注释*并选择一个名称-值对。
3. 单击*应用*。

在 **Active IQ Unified Manager** 中编辑注释规则

您可以编辑批注规则以修改条件组以及条件组内的条件，以便向存储对象添加批注或从中删除批注。

开始之前

您必须具有应用程序管理员或存储管理员角色。

编辑关联的标注规则时，标注将与存储对象分离。

步骤

1. 在左侧导航窗格中，单击 存储管理 > 注释。
2. 在*注释规则*选项卡中，选择要编辑的注释规则，然后单击*操作* > 编辑。
3. 在*编辑注释规则*对话框中，根据需要更改规则名称、注释名称和值、条件组和条件。

   您不能更改注释规则的目标对象类型。

4. 单击 **Save**。

在 **Active IQ Unified Manager** 中配置标注规则的条件

您可以配置一个或多个条件，以创建 Unified Manager 应用于存储对象的注释规则。符合注释规则的存储对象会使用规则中指定的值进行注释。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 存储管理 > 注释。
2. 在*注释规则*选项卡中，单击*添加*。
3. 在*添加注释规则*对话框中，输入规则的名称。
4. 从“目标对象类型”列表中选择一个对象类型，然后从列表中选择批注名称和值。
5. 在对话框的*条件*部分，从列表中选择操作数和运算符并输入条件值，或单击*添加条件*以创建新条件。
6. 单击*保存并添加*。

为批注规则配置条件的示例

考虑对象类型 SVM 的条件，其中对象名称包含“`svm_data`”。

请在添加注释规则对话框中执行以下步骤以配置条件：

步骤

1. 输入批注规则的名称。
2. 选择目标对象类型为 SVM。
3. 从注释列表中选择一个注释和一个值。
4. 在*条件*字段中，选择*对象名称*作为操作数。
5. 选择*包含*作为运算符。
6. 输入值为 `svm_data`。
7. 单击 **Add**。

删除 **Active IQ Unified Manager** 中的注释规则

当不再需要这些规则时，您可以从 Active IQ Unified Manager 中删除批注规则。

开始之前

您必须具有应用程序管理员或存储管理员角色。

删除注释规则后，注释将与存储对象解除关联并从中移除。

步骤

1. 在左侧导航窗格中，单击 存储管理 > 注释。
2. 在*注释规则*选项卡中，选择要删除的注释规则，然后单击*删除*。
3. 在*警告*对话框中，单击*是*确认删除。

在 **Active IQ Unified Manager** 中重新排列注释规则

您可以更改 Unified Manager 将批注规则应用于存储对象的顺序。批注规则会根据其排名按顺序应用于存储对象。配置批注规则时，其排名最低。但是，您可以根据要求更改批注规则的排名。

开始之前

您必须具有应用程序管理员或存储管理员角色。

您可以选择单行或多行，并执行许多拖放操作以更改批注规则的排名。但是，您必须保存更改，以便在批注规则选项卡中显示重新排序的优先级。

步骤

1. 在左侧导航窗格中，单击 存储管理 > 注释。
2. 在*注释规则*选项卡中，单击*重新排序*。
3. 在*重新排序标注规则*对话框中，拖放单行或多行以重新排列标注规则的顺序。
4. 单击 **Save**。

   您必须保存更改才能显示重新排序。

通过 **Web UI** 和维护控制台发送支持包

通过 **Active IQ Unified Manager** 的 **Web UI** 和维护控制台发送支持包

当您遇到的问题需要比 AutoSupport 消息提供更详细的诊断和故障排除时，您应该发送支持包。您可以使用 Unified Manager Web UI 和维护控制台向技术支持发送支持包。

Unified Manager 一次最多可存储两个完全支持捆绑包和三个轻量级支持捆绑包。

相关信息

"Unified Manager 用户角色和功能"

在 **Active IQ Unified Manager** 中向技术支持发送 **AutoSupport** 消息

通过 AutoSupport 页面，您可以向技术支持团队发送预定义和按需的 AutoSupport 消息，

以确保环境正常运行，并帮助您维护环境的完整性。默认情况下，AutoSupport 处于启用状态，不应将其禁用，以便您获得 NetAppActive IQ 的优势。

您可以根据需要在消息中发送有关 Unified Manager 服务器的诊断系统信息和详细数据，安排定期发送消息，甚至生成并向技术支持团队发送支持包。

> 具有存储管理员角色的用户可以生成按需 AutoSupport 消息和支持捆绑包并将其发送给技术支持。但是，只有管理员或维护用户才能启用或禁用定期 AutoSupport 并配置 HTTP 设置，如设置 HTTP 代理服务器一节所述。在需要使用 HTTP 代理服务器的环境中，应在存储管理员向技术支持发送按需 AutoSupport 消息和支持捆绑包之前完成配置。

发送按需 **AutoSupport** 消息

您可以生成按需消息并将其发送给技术支持人员、指定的电子邮件收件人或两者。

步骤

1. 导航至 常规 > **AutoSupport**，并执行以下一项或两项操作：
2. 如果要将 AutoSupport 消息发送给技术支持，请选中*发送给技术支持*复选框。
3. 如果要将 AutoSupport 消息发送给特定的电子邮件收件人，请选中 发送给电子邮件收件人 复选框，然后输入收件人的电子邮件地址。
4. 单击 **Save**。
5. 单击 生成并发送 **AutoSupport**。

启用定期 **AutoSupport**

您可以定期向技术支持发送特定的预定义消息，以进行问题诊断和解决。默认情况下，此功能处于启用状态。如果已禁用，管理员或维护用户可以启用这些设置。

步骤

1. 导航到*常规* > **AutoSupport**。
2. 在定期 AutoSupport 部分中，选中 启用定期向 **Active IQ** 发送 **AutoSupport** 数据 复选框。
3. 如果需要，请定义 HTTP 代理服务器的名称、端口和身份验证信息，如设置 HTTP 代理服务器一节所述。
4. 单击 **Save**。

上传按需支持包

您可以根据故障排除要求生成支持包并将其发送给技术支持。Unified Manager 仅存储最近生成的两个支持包。较早的支持包已从系统中删除。

由于某些类型的支持数据可能占用大量集群资源或需要很长时间才能完成，因此在选择完整支持捆绑包时，您可以包含或排除特定数据类型以减小支持捆绑包的大小。您还可以选择创建仅包含 30 天日志和配置数据库记录的轻量级支持捆绑包——它不包括性能数据、采集记录文件和服务器堆转储。

步骤

1. 导航到*常规* > **AutoSupport**。
2. 在按需支持捆绑包部分，单击*生成并发送支持捆绑包*。

3. 要向技术支持发送轻型支持捆绑包，请在生成和发送支持捆绑包弹出窗口中，选中生成轻型支持捆绑包复选框。
4. 或者，要发送完整支持捆绑包，请选中*生成完整支持捆绑包*复选框。选择要包含在支持捆绑包中或从中排除的特定数据类型。

   即使未选择任何数据类型，支持捆绑包仍会与其他 Unified Manager 数据一起生成。

5. 请选中 将捆绑包发送给技术支持 复选框，以生成捆绑包并将其发送给技术支持。如果不选中此复选框，则会生成捆绑包并将其本地存储在 Unified Manager 服务器中。生成的支持包可在 VMware 系统上的 /support 目录中、Linux 系统上的 `/opt/netapp/data/support/`中以及 Windows 系统上的 `ProgramData\NetApp\OnCommandAppData\ocum\support`中供以后使用。
6. 单击*发送*。

设置 **HTTP** 代理服务器

如果您的环境不提供从 Unified Manager 服务器的直接访问，您可以指定代理来提供 Internet 访问，以便向技术支持发送 AutoSupport 内容。此部分仅适用于管理员和维护用户。

- 使用 **HTTP** 代理

  选中此框以确定要用作 HTTP 代理的服务器。

  输入代理服务器的主机名或 IP 地址，以及用于连接到该服务器的端口号。

- 使用身份验证

  如果需要提供身份验证信息来访问用作 HTTP 代理的服务器，请选中此框。

  输入向 HTTP 代理进行身份验证所需的用户名和密码。

不支持仅提供基本身份验证的 HTTP 代理。

访问 **Active IQ Unified Manager** 中的维护控制台

如果 Unified Manager 用户界面未运行，或者需要执行用户界面中不可用的功能，则可以访问维护控制台来管理 Unified Manager 系统。

开始之前

您必须已安装并配置 Unified Manager。

15 分钟不活动后，维护控制台会将您注销。

在 VMware 上安装时，如果已经通过 VMware 控制台以维护用户身份登录，则不能同时使用 Secure Shell 登录。

步骤

1. 按照下面的步骤访问维护控制台：

在此操作系统上……	按照下面的步骤进行操作……
VMware	a. 使用 Secure Shell，连接到 Unified Manager 虚拟设备的 IP 地址或完全限定的域名。 b. 使用您的维护用户名和密码登录到维护控制台。
Linux	a. 使用 Secure Shell，连接到 Unified Manager 系统的 IP 地址或完全限定域名。 b. 使用维护用户 (umadmin) 名称和密码登录到此系统。 c. 输入命令 `maintenance_console`并按 Enter 键。
Windows	a. 使用管理员凭据登录到 Unified Manager 系统。 b. 以 Windows 管理员身份启动 PowerShell。 c. 输入命令 `maintenance_console`并按 Enter 键。

此时将显示 Unified Manager 维护控制台菜单。

从 **Active IQ Unified Manager** 生成并上传支持包

您可以生成包含诊断信息的支持包，以便将其发送到技术支持以获得故障排除帮助。

从 Unified Manager 9.8 开始，如果您的 Unified Manager 服务器已连接到互联网，您还可以从维护控制台向 NetApp 上传支持包。

开始之前

您必须能够以维护用户的身份访问维护控制台。

由于某些类型的支持数据可能会占用大量集群资源或需要很长时间才能完成，因此在选择完整支持包时，您可以指定要包含或排除的数据类型，以减小支持包的大小。您还可以选择创建一个仅包含 30 天日志和配置数据库记录的轻量级支持包——它不包含性能数据、采集记录文件和服务器堆转储。

Unified Manager 仅存储最近生成的两个支持捆绑包。较早的支持捆绑包将从系统中删除。

步骤

1. 在维护控制台*主菜单*中，选择*支持/诊断*。
2. 根据您希望在支持捆绑包中包含的详细信息级别，选择*生成轻量级支持捆绑包*或*生成支持捆绑包*。
3. 如果选择完整支持包，请选择或取消选择要在支持包中包含或排除的以下数据类型：

   - 数据库转储

     MySQL Server 数据库的转储。

   - 堆转储

     主要 Unified Manager 服务器进程的状态快照。此选项默认处于禁用状态，只有在客户支持提出请求时才应选择此选项。

◦ 采集记录

Unified Manager 与被监控集群之间的所有通信的记录。

如果取消选择所有数据类型，则仍会与其他 Unified Manager 数据一起生成支持包。

4. 键入 `g`，然后按 Enter 生成支持包。

由于生成支持捆绑包是一项内存密集型操作，因此系统会提示您确认此时是否确实要生成支持捆绑包。

5. 键入 `y`，然后按 Enter 生成支持捆绑包。

如果此时不想生成支持捆绑包，请键入 `n`，然后按 Enter。

6. 如果在完整支持捆绑包中包含了数据库转储文件，系统将提示您指定要包含性能统计信息的时间段。包含性能统计信息可能需要大量的时间和空间，因此您也可以在不包含性能统计信息的情况下转储数据库：

a. 以 YYYYMMDD 格式输入开始日期。

例如，输入 `20210101`表示 `2021` 年 `1` 月 `1` 日。如果不希望包含性能统计信息，请输入 `n`。

b. 输入要包括的统计天数，从指定开始日期的凌晨 12 点开始。

您可以输入一个从 1 到 10 的数字。

如果包含性能统计信息，系统将显示将收集性能统计信息的时间段。

7. 创建支持捆绑包后，系统会提示您是否要将其上传到 NetApp。键入 `y`，然后按 Enter。

系统会提示您输入支持案例编号。

8. 如果您已有案例编号，请输入该编号并按 Enter 键。否则，只需按 Enter 键。

支持包已上传到 NetApp。

如果您的 Unified Manager 服务器未连接到互联网，或者由于任何其他原因无法上传支持包，则可以检索并手动发送。您可以使用 SFTP 客户端或使用 UNIX 或 Linux CLI 命令检索它。在 Windows 安装中，可以使用远程桌面（RDP）检索支持包。

生成的支持捆绑包位于 VMware 系统上的 /support 目录、Linux 系统上的 /opt/netapp/data/support/ 以及 Windows 系统上的 ProgramData\NetApp\OnCommandAppData\ocum\support 中。

相关信息

"Unified Manager 用户角色和功能"

使用 **Windows** 客户端在 **Active IQ Unified Manager** 中检索支持包

如果您是 Windows 用户，可以下载并安装从 Unified Manager 服务器检索支持包的工具。您可以向技术支持发送支持包，以便更详细地诊断问题。Filezilla 或 WinSCP 是您可以使用的工具示例。

开始之前

您必须是维护用户才能执行此任务。

您必须使用支持 SCP 或 SFTP 的工具。

步骤

1. 下载并安装工具以检索支持包。
2. 打开工具。
3. 通过 SFTP 连接到 Unified Manager 管理服务器。

   该工具显示 /support 目录的内容，您可以查看所有现有的支持包。
4. 选择要复制的支持包的目标目录。
5. 选择要复制的支持捆绑包，并使用此工具将文件从 Unified Manager 服务器复制到本地系统。

使用 **UNIX** 或 **Linux** 客户端在 **Active IQ Unified Manager** 中检索支持包

如果您是 UNIX 或 Linux 用户，则可以使用 Linux 客户端服务器上的命令行界面 (CLI) 从您的 vApp 中检索支持包。您可以使用 SCP 或 SFTP 来检索支持包。

开始之前

您必须是维护用户才能执行此任务。

您必须已使用维护控制台生成支持包，并且支持包名称可用。

步骤

1. 使用 Linux 客户端服务器，通过 Telnet 或控制台访问 CLI。
2. 访问 `/support` 目录。
3. 检索支持包并使用以下命令将其复制到本地目录：

条件	命令
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>`

   使用维护控制台生成支持捆绑包时，会向您提供该支持捆绑包的名称。
4. 输入维护用户密码。

示例

以下示例使用 SCP 检索支持包：

```
        `$ 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
```

以下示例使用 SFTP 检索支持包：

```
        `$ 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
```

从 **Active IQ Unified Manager** 向技术支持发送支持包

如果问题需要比 AutoSupport 消息提供的更详细的诊断和故障排除信息，您可以向技术支持发送支持包。

开始之前

您必须能够访问支持包才能将其发送给技术支持。

您必须具有通过技术支持网站生成的案例编号。

步骤

1. 登录到 NetApp 支持站点。
2. 上传文件。

   "如何将文件上传至 NetApp"

与多个工作流程相关的任务和信息

了解 **Active IQ Unified Manager** 中的集群组件争用

当集群组件发生争用时，您可以识别集群性能问题。使用该组件的工作负载性能会下降，其对客户端请求的响应时间（延迟）会增加，这会在 Unified Manager 中触发事件。

处于争用状态的组件无法在最佳水平下运行。其性能会有所下降，并且其他集群组件和工作负载（称为 *victims* ）的性能可能会出现延迟增加的情况。要使组件摆脱争用状态，必须减少其工作负载或提高其处理更多工作的能力，以便性能能够恢复到正常水平。由于 Unified Manager 每隔五分钟收集并分析一次工作负载性能，因此它仅在集群组件被持续过度使用时才会检测到。在五分钟间隔内仅持续很短时间的暂时性过度使用峰值不会被检测到。

例如，存储聚合可能存在争用，因为其上的一个或多个工作负载正在争用以满足其 I/O 请求。聚合上的其他工作负载可能会受到影响，导致其性能下降。为了减少聚合上的活动量，您可以采取不同的步骤，例如将一个或多个

工作负载移动到不太繁忙的聚合或节点，以减少当前聚合的整体工作负载需求。对于 QoS 策略组，您可以调整吞吐量限制，或将工作负载移动到其他策略组，以便不再限制工作负载。

Unified Manager 可监控以下集群组件，以便在它们发生争用时向您发出警报：

- 网络

  表示集群上外部网络协议对 I/O 请求的等待时间。等待时间是指集群在对 I/O 请求做出响应前等待 “transfer ready” 事务完成的时间。如果网络组件存在争用，则意味着协议层的等待时间过长会影响一个或多个工作负载的延迟。

- 网络处理

  表示集群中涉及协议层和集群之间 I/O 处理的软件组件。自检测到事件以来，负责网络处理的节点可能已发生更改。如果网络处理组件处于争用状态，则意味着网络处理节点的高利用率正在影响一个或多个工作负载的延迟。

  在双活配置中使用全 SAN 阵列集群时，将显示两个节点的网络处理延迟值，以便您验证节点是否平均分担负载。

- 服务质量（**QoS**）上限

  表示分配给工作负载的存储服务质量（QoS）策略组的吞吐量最大值（峰值）设置。如果策略组组件存在争用，则表示策略组中的所有工作负载都受到设置的吞吐量限制的限制，这会影响其中一个或多个工作负载的延迟。

- **QoS** 限制下限

  表示分配给其他工作负载的 QoS 吞吐量最小（预期）设置导致的工作负载延迟。如果在某些工作负载上设置的 QoS 最小值使用了大部分带宽来保证承诺的吞吐量，则其他工作负载将受到限制并出现更高的延迟。

- 集群互连

  表示与已加入集群的节点物理连接的缆线和适配器。如果集群互连组件处于争用状态，则意味着在集群互连处等待 I/O 请求的时间较长，这会影响一个或多个工作负载的延迟。

- **Data Processing**

  表示集群中涉及集群和包含工作负载的存储聚合之间的 I/O 处理的软件组件。负责 Data Processing 的节点可能会在检测到事件后发生更改。如果 Data Processing 组件存在争用，则意味着 Data Processing 节点的高利用率会影响一个或多个工作负载的延迟。

- 卷激活

  表示跟踪所有活动卷使用情况的过程。在超过 1000 个卷处于活动状态的大型环境中，此过程将跟踪有多少关键卷需要同时通过节点访问资源。当并发活动卷的数量超过建议的最大阈值时，某些非关键卷将出现此处指出的延迟。

- **MetroCluster** 资源

  表示 MetroCluster 资源，包括 NVRAM 和交换机间链路（ISL），用于在 MetroCluster 配置中的集群之间镜像数据。如果 MetroCluster 组件存在争用，则意味着本地集群上工作负载的高写入吞吐量或链路运行状况问题正在影响本地集群上一个或多个工作负载的延迟。如果集群不在 MetroCluster 配置中，则不显示此图标。

- 聚合或 **SSD** 聚合操作

  表示运行工作负载的存储聚合。如果聚合组件存在争用，则意味着聚合的高利用率正在影响一个或多个工作负载的延迟。聚合由全部 HDD，或者 HDD 和 SSD 的混合（Flash Pool 聚合），或者 HDD 和云层的混合（FabricPool 聚合）组成。“SSD Aggregate” 由全部 SSD（全闪存聚合），或者 SSD 和云层的混合（FabricPool 聚合）组成。

- 云延迟

  表示集群和存储用户数据的云层之间的 I/O 处理所涉及的软件组件。如果云延迟组件发生争用，则意味着从云层上托管的卷进行的大量读取会影响一个或多个工作负载的延迟。

- 同步 **SnapMirror**

  表示集群中涉及在 SnapMirror 同步关系中将用户数据从主卷复制到辅助卷的软件组件。如果同步 SnapMirror 组件存在争用，则表示来自 SnapMirror 同步操作的活动正在影响一个或多个工作负载的延迟。

在 **Active IQ Unified Manager** 中查看卷/运行状况详细信息页面

您可以使用“卷/运行状况详细信息”页面查看有关所选卷的详细信息，例如容量、存储效率、配置、保护、注释和生成的事件。您还可以查看有关该卷的相关对象和相关警报的信息。

您必须具有应用程序管理员或存储管理员角色。

命令按钮

使用命令按钮可以对选定卷执行下列任务：

- 切换到性能视图

  使您能够导航到卷/性能详细信息页面。

- 操作

  - 添加警报

    用于向选定卷添加警报。

  - 编辑阈值

    用于修改选定卷的阈值设置。

  - 标注

    用于标注选定卷。

  - 保护

    用于为选定卷创建 SnapMirror 或 SnapVault 关系。

  - 关系

用于执行以下保护关系操作：

- 编辑

  启动“编辑关系”对话框，通过该对话框可以更改现有保护关系的现有 SnapMirror 策略、计划和最大传输速率。

- 中止

  中止选定关系正在进行的传输。（可选）通过此操作，您可以删除用于非基线传输的重新启动检查点。您无法删除用于基线传输的检查点。

- 暂停

  暂时禁用选定关系的计划更新。已在进行的传输必须在此关系暂停之前完成。

- 中断

  中断源卷和目标卷之间的关系并将目标更改为读写卷。

- 删除

  永久删除选定源和目标之间的关系。这些卷不会销毁，并且卷上的 Snapshot 副本不会删除。此操作无法撤消。

- 恢复

  启用已暂停的关系的计划传输。在下一个计划传输间隔会使用重新启动检查点（如果有）。

- 重新同步

  用于重新同步之前已断开的关系。

- 初始化/更新

  用于对新的保护关系执行首次基线传输，或者如果该关系已初始化，则用于执行手动更新。

- 反向重新同步

  用于重新建立之前已断开的保护关系，通过将源设为原始目标的副本反转源和目标的功能。源上的内容将被目标上的内容覆盖，晚于通用 Snapshot 副本中的数据的任何数据都将被删除。

◦ 还原

用于将数据从一个卷还原到另一个卷。有关信息，请参见 "使用卷/运行状况详细信息页面还原数据"。

对于处于同步保护关系的卷，“还原”按钮和“关系”操作按钮将不可用。

- 查看卷

使您能够导航到运行状况：所有卷视图。

“容量”选项卡会显示有关所选卷的详细信息，例如其物理容量、逻辑容量、阈值设置、配额容量以及有关任何卷移动操作的信息：

- 物理容量

  详细描述卷的物理容量：

  - Snapshot 溢出

    显示 Snapshot 副本占用的数据空间。

  - 已用

    显示卷中数据的已用空间。

  - 警告

    指示卷中的空间接近全满。如果违反此阈值，则会生成“空间接近全满”事件。

  - 错误

    指示卷中的空间全满。如果违反此阈值，则会生成“空间已满”事件。

  - 不可用

    指示生成了“精简配置卷空间存在风险”事件，精简配置卷中的空间由于聚合容量问题而存在风险。只有精简配置卷才会显示不可用容量。

  - 数据图形

    显示卷的总数据容量和已使用数据容量。

    如果启用了自动增长，则数据图形还会显示聚合中的可用空间。数据图形显示卷中的数据可以使用的有效存储空间，可以是以下容量之一：

    - 下列情况下卷的实际数据容量：
      - 禁用了“自动增长”。
      - 启用了“自动增长”的卷已达到大小上限。
      - 启用了“自动增长”的厚配置卷无法再继续增长。
    - 在考虑了卷大小上限之后的卷数据容量（适用于精简配置的卷以及在聚合中的空间允许卷达到大小上限时适用于厚配置卷）
    - 在考虑下一个可能的自动增长大小之后的卷数据容量（适用于具有自动增长百分比阈值的厚配置卷）

  - Snapshot 副本图形

    只有已使用的 Snapshot 容量或 Snapshot 预留不为零时，才会显示此图形。

如果已使用的 Snapshot 容量超出 Snapshot 预留，则两个图形都会显示超出 Snapshot 预留的 Snapshot 容

量。

- 容量逻辑

  显示卷的逻辑空间特征。逻辑空间表示磁盘上所存储数据的实际大小，而不是使用 ONTAP 存储效率技术节省的空间。

  - 逻辑空间报告

    显示卷是否配置了逻辑空间报告。该值可以为 Enabled、Disabled 或 Not applicable。对于较旧版本的 ONTAP 或不支持逻辑空间报告的卷，将显示 “Not applicable”。

  - 已用

    根据总数据容量显示卷中的数据所使用的逻辑空间量和已用逻辑空间的百分比。

  - 强制实施逻辑空间

    显示是否为精简配置卷配置逻辑空间强制实施。如果设置为“已启用”，则卷的逻辑已用容量不能大于当前设置的物理卷容量。

- 自动增长

  显示卷在空间不足的情况下是否会自动增长。

- 空间保证

  显示在卷从聚合中删除可用块时的 FlexVol 卷设置控制。这样可以保证这些块可写入卷中的文件。空间保证可设置为下列各项之一：

  - 无

    不为卷配置任何空间保证。

  - 文件

    保证稀疏写入文件（例如 LUN）的完整大小。

  - 卷

    保证卷的完整大小。

  - 部分

    FlexCache 卷根据其大小保留空间。如果 FlexCache 卷的大小为 100 MB 或更大，则默认情况下最小空间保证设置为 100 MB。如果 FlexCache 卷的大小小于 100 MB，则最小空间保证设置为 FlexCache 卷的大小。如果 FlexCache 卷的大小稍后增加，则最小空间保证不会增加。

    卷的类型为“数据缓存”时，空间保证为“部分”。

- 详细信息（物理）

显示卷的物理特征。

- 总容量

  显示卷的总物理容量。

- 数据容量

  显示卷使用的物理空间量（已用容量）以及卷中仍然可用的物理空间量（可用容量）。这些值还以总物理容量的百分比形式显示。

  为精简配置卷生成“精简配置卷空间存在风险”事件时，将显示卷使用的空间量（已用容量）以及卷中可用、但由于聚合容量问题无法使用的空间量（不可用容量）。

- **Snapshot** 预留

  显示 Snapshot 副本使用的空间量（已用容量）以及可供卷中 Snapshot 副本使用的空间量（可用容量）。这些值还以 Snapshot 预留总容量的百分比形式显示。

  为精简配置卷生成“精简配置卷空间存在风险”事件时，将显示 Snapshot 副本使用的空间量（已用容量）以及卷中可用、但由于聚合容量问题无法用于创建 Snapshot 副本的空间量（不可用容量）。

- 卷阈值

  显示下列卷容量阈值：

  - 接近全满阈值

    指定卷接近全满时的百分比。

  - 全满阈值

    指定卷全满时的百分比。

- 其他详细信息

  - 自动增长大小上限

    显示卷可以自动增长到的大小上限。默认值为卷在创建时的大小的 120%。只有在已为卷启用了自动增长时才会显示此字段。

  - qtree 配额已提交的容量

    显示配额中预留的空间。

  - qtree 配额已过量提交的容量

    显示在系统生成“卷 qtree 配额已过量提交”事件之前可以使用的空间量。

  - 预留百分比

    控制覆盖预留的大小。默认情况下，预留百分比设置为 100，表示会预留全部所需预留空间，从而可以使对象受到全面保护，以免被覆盖。如果预留百分比小于 100%，则为该卷中所有预留空间的文件预留

的空间会减少至该预留百分比。

- Snapshot 每日增长率

  显示选定卷中 Snapshot 副本每 24 小时发生的更改（以百分比或 KB、MB、GB 等表示）。

- Snapshot 达到全满前的天数

  显示为卷中 Snapshot 副本预留的空间达到指定阈值前的预计剩余天数。

  在卷中 Snapshot 副本的增长率为零或负数或者没有足够的数据用来计算增长率时，“Snapshot 达到全满前的天数”字段将显示值“不适用”。

- Snapshot 自动删除

  指定在对卷执行的写入因聚合中空间不足而失败时是否自动删除 Snapshot 副本以释放空间。

- Snapshot 副本

  显示有关卷中 Snapshot 副本的信息。

  卷中的 Snapshot 副本数将显示为链接。单击此链接将打开“卷上的 Snapshot Copies”对话框，其中显示 Snapshot 副本的详细信息。

Snapshot 副本计数大约每小时更新一次，但 Snapshot 副本列表仅在您单击该图标时才进行更新。这可能会造成拓扑中显示的 Snapshot 副本计数不同于您单击该图标时列出的 Snapshot 副本数量。

- 卷移动

  显示当前或最近对卷执行的卷移动操作的状态以及其他详细信息，例如正在进行的卷移动操作目前所处的阶段、源聚合、目标聚合、开始时间、结束时间以及估计结束时间。

  还显示在所选卷上执行的卷移动操作的数量。您可以通过单击*卷移动历史记录*链接查看有关卷移动操作的更多信息。

配置选项卡

“配置”选项卡显示有关所选卷的详细信息，例如卷的导出策略、RAID 类型、容量和存储效率相关功能：

- 概述

  - 全名

    显示卷的全名。

  - 聚合

    显示卷所在的聚合的名称或 FlexGroup 卷所在的聚合的数量。

  - 分层策略

    显示为卷设置的分层策略；如果卷部署在已启用 FabricPool 的聚合上。此策略可以为“无”、“仅 Snapshot”、“备份”、“自动”或“全部”。

- Storage VM

  显示包含卷的 SVM 的名称。

- 接合路径

  显示路径的状态，该路径可以是活动的或非活动的。此时也会显示卷挂载到的 SVM 中的路径。您可以单击*历史记录*链接以查看对接合路径的最近五次更改。

- 导出策略

  显示为卷创建的导出策略的名称。您可以单击此链接，查看有关导出策略、身份验证协议以及在属于 SVM 的卷上启用的访问权限的详细信息。

- 模式

  显示卷模式。卷模式可以为“FlexVol”或“FlexGroup”。

- 类型

  显示选定卷的类型。卷类型可以为“读写”、“负载共享”、“数据保护”、“数据缓存”或“临时”。

- RAID 类型

  显示选定卷的 RAID 类型。RAID 类型可以为“RAID0”、“RAID4”或“RAID-DP”或“RAID-TEC”。

  可能会为 FlexGroup 卷显示多种 RAID 类型，因为 FlexGroup 的成分卷可能位于不同类型的聚合上。

- SnapLock 类型

  显示卷所在聚合的 SnapLock 类型。

- SnapLock 过期时间

  显示 SnapLock 卷的过期日期。

- 容量
  - 精简配置

    显示是否为卷配置了精简配置。

  - 自动增长

    显示灵活卷是否在聚合内自动增长。

  - Snapshot 自动删除

    指定在对卷执行的写入因聚合中空间不足而失败时是否自动删除 Snapshot 副本以释放空间。

  - 配额

指定是否为卷启用了配额。

- 效率
  - 数据压缩

    指定是启用还是禁用压缩。

  - 重复数据删除

    指定是启用还是禁用重复数据删除。

  - 重复数据删除模式

    指定对卷启用的重复数据删除操作是手动操作、计划操作，还是基于策略的操作。如果模式设置为“已计划”，则显示操作计划；如果模式设置为某种策略，则显示策略名称。

  - 重复数据删除类型

    指定在卷上运行的重复数据删除操作的类型。如果卷处于某种 SnapVault 关系中，则显示的类型为“SnapVault”。对于任何其他卷，类型显示为“常规”。

  - 存储效率策略

    指定已通过 Unified Manager 分配给此卷的存储效率策略的名称。此策略可以控制压缩和重复数据删除设置。

- 保护
  - Snapshot 副本

    指定是启用还是禁用了自动 Snapshot 副本。

保护选项卡

“保护”选项卡显示有关所选卷的保护详细信息，例如延迟信息、关系类型和关系的拓扑。

- 摘要

  显示所选卷的保护关系（SnapMirror、SnapVault 或 Storage VM DR）属性。对于任何其他关系类型，仅显示 Relationship Type 属性。如果选择了主卷，则仅显示托管和本地 Snapshot 副本策略。为 SnapMirror 和 SnapVault 关系显示的属性包括以下内容：

  - 源卷

    如果选定卷是目标，则显示该卷的源的名称。

  - 滞后状态

    显示保护关系的更新或传输滞后状态。状态可以是“错误”、“警告”或“严重”。

    滞后状态不适用于同步关系。

  - 滞后持续时间

显示镜像中的数据滞后于源的时间。

- 上次成功更新

  显示最近成功更新保护关系的日期和时间。

  上次成功更新不适用于同步关系。

- 存储服务成员

  显示对于卷是否属于存储服务以及由存储服务所托管的选择是“是”还是“否”。

- 版本灵活的复制

  显示“是”、“是，使用备份选项”或“无”。“是”指示即使源和目标卷运行不同版本的 ONTAP 软件，也有可能进行 SnapMirror 复制。“是，使用备份选项”指示实施 SnapMirror 保护并且能够将多个版本的备份副本保留在目标上。“无”指示“版本灵活的复制”未启用。

- 关系功能

  指示可用于保护关系的 ONTAP 功能。

- 保护服务

  如果关系由保护合作伙伴应用程序托管，则显示保护服务的名称。

- 关系类型

  显示任何关系类型，包括异步镜像、异步存储、异步 MirrorVault、StrictSync 和同步。

- 关系状况

  显示 SnapMirror 或 SnapVault 关系的状况。该状况可以是“未初始化”、“已执行 SnapMirror”或“已断开”。如果选择源卷，则关系状况不适用，也不会显示。

- 传输状态

  显示保护关系的传输状态。传输状态可以是下列状态之一：

  - 正在中止

    SnapMirror 传输已启用；但是，正在执行一个传输中止操作，此操作可能需要删除检查点。

  - 正在检查

    正在对目标卷进行诊断检查，当前未进行传输。

  - 正在完成

    SnapMirror 传输已启用。卷当前处于增量 SnapVault 传输的传输后阶段。

  - 闲置

已启用传输，但当前未进行传输。

- 同步

  处于同步关系的两个卷中的数据处于同步状态。

- 不同步

  目标卷中的数据与源卷不同步。

- 正在准备

  SnapMirror 传输已启用。卷当前处于增量 SnapVault 传输的传输前阶段。

- 已排队

  SnapMirror 传输已启用。当前未进行传输。

- 已暂停

  SnapMirror 传输已禁用。当前未进行传输。

- 正在暂停

  正在进行 SnapMirror 传输。其他传输已禁用。

- 正在传输

  已启用 SnapMirror 传输，且传输正在进行中。

- 正在过渡

  从源卷到目标卷的异步数据传输完成，并且已开始过渡到同步操作。

- 正在等待

  SnapMirror 传输已启动，但某些关联任务正在等待排队。

◦ 最大传输速率

显示关系的最大传输速率。最大传输速率可能是以 KB/秒 (Kbps)、MB/秒 (Mbps)、GB/秒 (Gbps) 或 TB/秒 (Tbps) 为单位的数值。如果显示“无限制”，则关系之间的基线传输无限制。

◦ SnapMirror 策略

显示卷的保护策略。DPDefault 表示默认异步镜像保护策略，XDPDefault 表示默认异步保管库策略，DPSyncDefault 表示默认异步 MirrorVault 策略。StrictSync 表示默认同步严格保护策略，Sync 表示默认同步策略。您可以单击策略名称以查看与该策略关联的详细信息，包括以下信息：

- 传输优先级
- 忽略访问时间设置
- 尝试次数限制

- 注释
- SnapMirror 标签
- 保留设置
- 实际 Snapshot 副本
- 保留 Snapshot 副本
- 保留警告阈值
- 无保留设置的快照副本 在源为数据保护（DP）卷的级联 SnapVault 关系中，仅适用规则“`sm_created`”。

◦ 更新计划

显示分配给关系的 SnapMirror 计划。将光标置于信息图标上方可以显示计划详细信息。

◦ 本地 Snapshot 策略

显示卷的 Snapshot 副本策略。策略可以是“默认”、“无”或者是为自定义策略指定的任何名称。

◦ 受保护于

显示用于所选卷的保护类型。例如，如果卷受一致性组和 SnapMirror 卷关系保护，则此字段会同时显示 SnapMirror 和一致性组。此字段还提供了一个链接，将您重定向到“关系”页面以查看统一的关系状态。此链接仅适用于组成关系。

◦ 一致性组

对于受 SnapMirror 活动同步关系保护的卷，此列显示卷的一致性组。

- 视图

显示选定卷的保护拓扑。拓扑包含与选定卷相关的所有卷的图形表示。选定卷以深灰色框表示，拓扑中卷之间的直线表示保护关系类型。拓扑中的关系方向是按从左到右显示，每个关系的源在左侧，目标在右侧。

双粗线表示异步镜像关系，单粗线表示异步 Vault 关系，双细线表示异步 MirrorVault 关系，粗线和细线表示同步关系。下表指明同步关系是 StrictSync 还是 Sync。

右键单击某个卷将显示一个菜单，从中可以选择保护该卷或将数据还原到该卷。右键单击某个关系将显示一个菜单，从中可以选择编辑、中止、暂停、中断、删除或恢复关系。

在以下情况下，不会显示菜单：

◦ RBAC 设置不允许执行此操作，例如您只有操作员权限

◦ 卷处于同步保护关系

◦ 当卷 ID 未知时，例如，当您具有集群间关系并且尚未发现目标集群时，单击拓扑中的另一个卷将选择并显示该卷的信息。卷左上角的问号（ ）表示该卷缺失或尚未被发现。这也可能表明容量信息缺失。将光标悬停在问号上会显示其他信息，包括补救措施建议。

如果拓扑符合几个常用拓扑模板之一，则会显示有关卷容量、滞后、Snapshot 副本及上次成功传输数据的信息。如果拓扑不符合这些模板之一，则有关卷滞后及上次成功传输数据的信息将显示在拓扑下面的关系表中。在这种情况下，表中突出显示的行指示选定卷，而在拓扑视图中，有蓝点的粗线指示选定卷与其源卷之间的关系。

拓扑视图包含下列信息：

- 容量

  显示卷使用的总容量。将光标置于拓扑中的某个卷上，会在“当前阈值设置”对话框中显示该卷的当前警告和严重阈值设置。您还可以通过单击“当前阈值设置”对话框中的*编辑阈值*链接来编辑阈值设置。清除*容量*复选框将隐藏拓扑中所有卷的所有容量信息。

- 滞后

  显示传入保护关系的延迟持续时间和延迟状态。清除*延迟*复选框会隐藏拓扑中所有卷的所有延迟信息。当*延迟*复选框变暗时，所选卷的延迟信息以及所有相关卷的延迟信息将显示在拓扑下方的关系表中。

- Snapshot

  显示可用于卷的 Snapshot 副本数。清除 **Snapshot** 复选框将隐藏拓扑中所有卷的所有 Snapshot 副本信息。单击 Snapshot 副本图标（）将显示卷的 Snapshot 副本列表。图标旁边显示的 Snapshot 副本计数大约每小时更新一次；但是，Snapshot 副本列表会在单击图标时更新。这可能会导致拓扑中显示的 Snapshot 副本计数与单击图标时列出的 Snapshot 副本数之间存在差异。

- 上次成功传输

  显示上次成功数据传输的数据量、持续时间、时间和日期。当 上次成功传输 复选框灰显时，所选卷的上次成功传输信息以及所有相关卷的上次成功传输信息将显示在拓扑下方的关系表中。

    - 历史记录

      在图形中显示所选卷的传入 SnapMirror 和 SnapVault 保护关系的历史记录。有三种历史记录图可用：传入关系延迟持续时间、传入关系传输持续时间和传入关系传输大小。仅当您选择目标卷时，才会显示历史记录信息。如果选择主卷，则图形为空，并显示消息“未找到数据”。如果卷受一致性组和 SnapMirror 同步关系保护，则不会显示关系传输持续时间和关系传输大小的信息。

  您可以从“历史记录”窗格顶部的下拉列表中选择图形类型。您也可以选择 1 周、1 个月或 1 年，查看特定时间段的详细信息。历史图表可以帮助您识别趋势：例如，如果在一天或一周的同一时间传输大量数据，或者持续超出滞后警告或滞后错误阈值，您可以采取适当的措施。此外，您可以单击 导出 按钮，为您正在查看的图表创建 CSV 格式的报告。

保护历史记录图显示下列信息：

- 关系滞后持续时间

  在纵轴 (y) 上显示秒数、分钟数或小时数，在横轴 (x) 上显示天数、月数或年数，具体取决于选定的持续时间段。y 轴上的最大值表示在 x 轴上所显示的持续时间段内达到的最大滞后持续时间。图形中的橙色水平线表示滞后错误阈值，黄色水平线表示滞后警告阈值。将光标置于这些线上方可以显示阈值设置。蓝色水平线表示滞后持续时间。可以通过将光标置于感兴趣区域上方来查看图中特定点的详细信息。

- 关系转移持续时间

  在纵轴 (y) 上显示秒数、分钟数或小时数，在横轴 (x) 上显示天数、月数或年数，具体取决于选定的持续时间段。y 轴上的最大值表示在 x 轴上所显示的持续时间段内达到的最大传输持续时间。可以通过将光标置于感兴趣区域上方来查看图中特定点的详细信息。

  对于处于同步保护关系中的卷，不会显示此图表。

- 关系传输大小

  根据传输大小在纵轴 (y) 上显示字节数、千字节数、兆字节数等数字，根据选定时间段在横轴 (x) 上显示天数、月数或年数。y 轴上的最大值表示在 x 轴上所显示的持续时间段内达到的最大传输大小。可以通过将光标置于感兴趣区域上方来查看图中特定点的详细信息。

  对于处于同步保护关系中的卷，不会显示此图表。

历史记录区域

历史记录区域显示图形，提供有关选定卷的容量和空间预留的信息。此外，您可以点击*导出*按钮，以 CSV 格式为您正在查看的图表创建报告。

当数据或卷的状态在一段时间内保持不变时，图形可能为空，并且会显示“未找到数据”消息。

您可以从“历史记录”窗格顶部的下拉列表中选择图形类型。您也可以选择 1 周、1 个月或 1 年，查看特定时间段的详细信息。历史记录图表可以帮助您识别趋势——例如，如果卷使用量始终突破“几乎已满”阈值，您可以采取适当的操作。

历史记录图显示下列信息：

- 已用卷容量

  在纵轴 (y) 上以折线图的形式显示卷中的已用容量和基于使用情况历史记录使用卷容量的趋势（以字节、千字节、兆字节等表示）。时间段显示在横轴 (x) 上。您可以选择一周、一个月或一年作为时间段。可以通过将光标置于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击“已用卷容量”图例时，“已用卷容量”图形线条处于隐藏状态。

- 已用卷容量与总卷容量

  在纵轴 (y) 上以折线图的形式显示基于使用情况历史记录使用卷容量的趋势，以及已用容量、总容量和通过重复数据删除和数据压缩节省的空间的详细信息（以字节、千字节、兆字节等表示）。时间段显示在横轴 (x) 上。您可以选择一周、一个月或一年作为时间段。可以通过将光标置于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击“Trend Capacity Used”图例时，“Trend Capacity Used”图形线条处于隐藏状态。

- 已用卷容量（%）

  在纵轴 (y) 上以折线图的形式显示卷中的已用容量和基于使用情况历史记录使用卷容量的趋势（以百分比表示）。时间段显示在横轴 (x) 上。您可以选择一周、一个月或一年作为时间段。可以通过将光标置于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击“已用卷容量”图例时，“已用卷容量”图形线条处于隐藏状态。

- 已用快照容量（%）

  在纵轴 (y) 上以折线图的形式显示 Snapshot 预留和 Snapshot 警告阈值，并以面积图的形式显示 Snapshot 副本使用的容量。Snapshot 溢出用不同的颜色表示。时间段显示在横轴 (x) 上。您可以选择一周、一个月或一年作为时间段。可以通过将光标置于特定区域上方来查看图中特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，单击“Snapshot 预留”图例时，“Snapshot 预留”图形线条处于隐藏状态。

事件列表

“事件”列表显示有关新事件和已确认事件的详细信息：

- 严重程度

  显示事件的严重级别。

- 事件

  显示事件名称。

- 触发时间

  显示自事件生成以来经过的时间。如果经过的时间超过一周，则显示生成事件时的时间戳。

相关标注窗格

通过“相关批注”窗格，您可以查看与所选卷关联的批注详细信息。详细信息包括应用于卷的批注名称和批注值。您还可以从“相关批注”窗格中删除手动批注。

相关设备窗格

使用“相关设备”窗格，您可以查看并导航到与卷相关的 SVM、聚合、qtree、LUN 和 Snapshot 副本：

- **Storage Virtual Machine**

  显示包含所选卷的 SVM 的容量和运行状况状态。

- 聚合

  显示选定卷所在聚合的容量和运行状况。对于 FlexGroup 卷，列出包含 FlexGroup 的聚合数。

- 聚合中的卷

  显示属于选定卷父聚合的所有卷的数量和容量。此外，系统还将基于最高严重性级别显示卷的运行状况。例如，如果一个聚合包含十个卷，其中五个显示“警告”状态，其余五个显示“严重”状态，则显示的状态为“严重”。对于 FlexGroup 卷，不会显示此组件。

- **Qtrees**

  显示选定卷包含的 qtree 数量以及选定卷包含的具有配额的 qtree 容量。系统将相对于卷数据容量来显示具有配额的 qtree 容量。此外，系统还将基于最高严重性级别显示 qtree 的运行状况。例如，如果一个卷有十个 qtree，五个为“警告”状态，其余五个为“严重”状态，则显示的状态为“严重”。

- **NFS** 共享

  显示与卷关联的 NFS 共享的数量和状态。

- **SMB** 共享

  显示 SMB/CIFS 共享的数量和状态。

- **LUN**

  显示选定卷中所有 LUN 的数量和总大小。此外，系统还将基于最高严重性级别显示 LUN 的运行状况。

- 用户和组配额

  显示与卷及其 qtree 关联的用户和用户组配额的数量和状态。

- **FlexClone** 卷

  显示选定卷的所有克隆卷的数量和容量。只有当选定卷包含克隆卷时，才会显示此数量和容量。

- 父卷

  显示选定 FlexClone 卷的父卷的名称和容量。只有当选定卷为 FlexClone 卷时，才会显示父卷。

相关组窗格

“相关组”窗格用于查看与所选卷关联的组列表。

相关警报窗格

“相关警报”窗格用于查看为选定卷创建的警报列表。您还可以通过单击“添加警报”链接来添加警报，或通过单击警报名称来编辑现有警报。

在 **Active IQ Unified Manager** 中查看 **Storage VM /** 运行状况详细信息页面

您可以使用 Storage VM / 运行状况详细信息页面查看有关所选 Storage VM 的详细信息，例如其运行状况、容量、配置、数据策略、逻辑接口（LIF）、LUN、qtree、用户、用户组配额和保护详细信息。您还可以查看有关 Storage VM 的相关对象和相关警报的信息。

您只能监控数据存储 VM。

命令按钮

通过命令按钮，您可以为选定的存储 VM 执行以下任务：

- 切换到性能视图

  使您能够导航到 Storage VM / 性能详细信息页面。

- 操作
  - 添加警报

    使您能够向选定的 storage VM 添加警报。

  - 标注

    使您能够注释选定的 storage VM。

- 查看 **Storage VM**

使您能够导航到运行状况：所有 Storage VM 视图。

运行状况选项卡

“运行状况”选项卡显示有关各种对象（如卷、聚合、NAS LIF、SAN LIF、LUN、协议、服务、NFS 共享和 CIFS 共享）的数据可用性、数据容量和保护问题的详细信息。

您可以单击某个对象的图形来查看经过筛选的对象列表。例如，可以单击显示警告的卷容量图形来查看容量问题的严重性为“警告”的卷列表。

- 可用性问题

  以图形形式显示对象的总数，包括存在可用性问题的对象和不存在任何可用性相关问题的对象。图中的颜色表示问题的不同严重程度。图表下方的信息提供了有关可能影响或已经影响存储 VM 中数据可用性的可用性问题的详细信息。例如，显示有关已关闭的 NAS LIF 和 SAN LIF 以及离线的卷的信息。

  此外，您还可以查看有关当前正在运行的相关协议和服务以及 NFS 和 CIFS 共享的数量和状态的信息。

- 容量问题

  以图形形式显示对象总数，包括存在容量问题的对象和不存在任何与容量相关问题的对象。图中的颜色表示问题的不同严重程度。图表下方的信息提供了有关可能影响或已经影响 storage VM 中数据容量的容量问题的详细信息。例如，显示有关可能超出设定阈值的聚合的信息。

- 保护问题

  通过将关系总数显示为字段对话框，提供与存储虚拟机保护相关的运行状况的快速概述，包括存在保护问题的关系和不存在任何保护相关问题的关系。您还可以查看选定存储虚拟机的存储虚拟机 DR 关系的状态。此处显示存储虚拟机 DR 关系事件，单击这些事件将转到事件详细信息页面。当存在未受保护的卷时，单击该链接将转到“运行状况：所有卷”视图，您可以在其中查看存储虚拟机上未受保护卷的过滤列表。图中的颜色表示问题的不同严重程度。单击图表将转到“关系：所有关系”视图，您可以在其中查看保护关系详细信息的筛选列表。图表下方的信息提供了有关可能影响或已经影响存储虚拟机中数据保护的保护问题的详细信息。例如，显示有关 Snapshot 副本预留量接近满的卷的信息或有关 SnapMirror 关系滞后问题的信息。

容量选项卡

Capacity 选项卡显示有关选定 SVM 的数据容量的详细信息。

对于带有 FlexVol 卷或 FlexGroup 卷的 Storage VM，将显示以下信息：

- 容量

  “容量”区域显示有关从所有卷中分配的已用容量和可用容量的详细信息：

  - 总容量

    显示 Storage VM 的总容量。

  - 已用

    显示属于 Storage VM 的卷中的数据所使用的空间。

  - 保证可用

显示 Storage VM 中可用于卷的数据的保证可用空间。

- 无保证

显示 Storage VM 中为精简配置卷分配的数据的剩余可用空间。

- 存在容量问题的卷

“存在容量问题的卷”列表以表格形式显示有关具有容量问题的卷的详细信息：

- 状态

指示卷存在额定严重性的容量相关问题。

可以将指针移动到状态上方来查看针对该卷生成的一个或多个事件的详细信息。

如果卷的状态由单个事件确定，您可以查看事件名称、触发事件的时间和日期、获分配该事件的管理员名称以及事件原因等信息。您可以使用*查看详细信息*按钮查看有关该事件的更多信息。

如果卷的状态由相同严重程度的多个事件确定，则将显示前三个事件，其中包含事件名称、事件触发的时间和日期以及分配事件的管理员的名称等信息。您可以通过单击事件名称查看有关这些事件的更多详细信息。您还可以单击 查看所有事件 链接以查看生成的事件列表。

一个卷可以具有多个严重性相同或不同的事件。但是，系统将仅显示最高严重性。例如，如果卷具有严重性为“错误”和“警告”的两个事件，则仅显示“错误”严重性。

- 卷

显示卷的名称。

- 已用数据容量

以图形方式显示卷容量使用量（百分比）的信息。

- 达到全满前的天数

显示在卷容量达到全满前的预计剩余天数。

- 精简配置

显示是否已为选定卷设置空间保证。有效值为“是”或“否”。

- 聚合

对于 FlexVol 卷，显示该卷所在聚合的名称。对于 FlexGroup 卷，显示 FlexGroup 中使用的聚合数。

配置选项卡

“配置”选项卡显示有关所选存储虚拟机的配置详细信息，例如其群集、根卷、其包含的卷类型（FlexVol 卷）、策略以及在存储虚拟机上创建的保护：

- 概述
  - 集群

显示存储 VM 所属集群的名称。

- 允许的卷类型

  显示可在存储 VM 中创建的卷类型。类型可以是 FlexVol 或 FlexVol/FlexGroup。

- 根卷

  显示存储 VM 的根卷名称。

- 允许的协议

  显示可以在存储 VM 上配置的协议类型。此外，还指示协议是已启动（）、已停止（）还是未配置（）。

- 数据网络接口
  - NAS

    显示与 storage VM 关联的 NAS 接口数。此外，还指示接口是已启动（）还是已关闭（）。

  - SAN

    显示与 storage VM 关联的 SAN 接口数。此外，还指示接口是已启动（）还是已关闭（）。

  - FC-NVMe

    显示与 Storage VM 关联的 FC-NVMe 接口的数量。此外，还指示接口是已启动（）还是已关闭（）。

- 管理网络接口
  - 可用性

    显示与 Storage VM 关联的管理接口数。此外，还指示管理接口是已启动（）还是已关闭（）。

- 策略
  - Snapshot

    显示在 Storage VM 上创建的 Snapshot 策略的名称。

  - 导出策略

    如果仅创建了一个策略，则显示该导出策略的名称；如果创建了多个策略，则显示导出策略的数量。

- 保护
  - Storage VM 灾难恢复

    显示所选存储虚拟机是受保护、目标还是未受保护，以及保护该存储虚拟机的目标名称。如果选定的存储虚拟机是目标，则显示源存储虚拟机的详细信息。在扇出情况下，此字段显示保护该存储虚拟机的目标存储虚拟机总数。计数链接将带您进入按源存储虚拟机筛选的存储虚拟机关系网格。

  - 受保护的卷

显示所选存储 VM 上受保护卷在总卷中的数量。如果您正在查看目标存储 VM，则数字链接适用于所选存储 VM 的目标卷。

- 未受保护的卷

  显示选定存储虚拟机上未受保护的卷数。

- 服务
  - 类型

    显示在存储虚拟机上配置的服务类型。类型可以是域名系统（DNS）或网络信息服务（NIS）。

  - 州/省

    显示服务的状态，可以是 Up（）、Down（）或 Not Configured（）。

  - 域名

    对于 DNS 服务，显示 DNS 服务器的完全限定域名 (FQDN)；对于 NIS 服务，显示 NIS 服务器的完全限定域名 (FQDN)。如果启用了 NIS 服务器，则显示 NIS 服务器的活动 FQDN。如果禁用了 NIS 服务器，则显示所有 FQDN 的列表。

  - IP 地址

    显示 DNS 或 NIS 服务器的 IP 地址。如果启用了 NIS 服务器，则显示 NIS 服务器的活动 IP 地址。如果禁用了 NIS 服务器，则显示所有 IP 地址的列表。

网络接口选项卡

“网络接口”选项卡显示有关在选定存储 VM 上创建的数据网络接口（LIF）的详细信息：

- 网络接口

  显示在所选存储 VM 上创建的接口的名称。

- 运行状态

  显示接口的运行状态，可以是 Up （）、Down （）或 Unknown （）。接口的运行状态取决于其物理端口的状态。

- 管理状态

  显示接口的管理状态，可以是 Up（）、Down（）或 Unknown（）。接口的管理状态由存储管理员控制，以便对配置进行更改或用于维护目的。管理状态可以与操作状态不同。但是，如果接口的管理状态为 Down，则默认情况下运行状态为 Down。

- **IP** 地址 **/ WWPN**

  显示以太网接口的 IP 地址和 FC LIF 的全球通用端口名称 (WWPN)。

- 协议

显示为接口指定的数据协议（例如 CIFS、NFS、iSCSI、FC/FCoE、FC-NVMe 和 FlexCache）的列表。

- 角色

  显示接口角色。角色可以是“数据”或“管理”。

- 主端口

  显示最初与接口关联的物理端口。

- 当前端口

  显示当前与接口关联的物理端口。如果接口已迁移，则当前端口可能与主端口不同。

- 端口集

  显示接口所映射到的端口集。

- 故障转移策略

  显示为接口配置的故障转移策略。对于 NFS、CIFS 和 FlexCache 接口，默认故障转移策略为“下一个可用”。故障转移策略不适用于 FC 和 iSCSI 接口。

- 路由组

  显示路由组的名称。可以单击路由组名称来查看有关路由和目标网关的详细信息。

  ONTAP 8.3 或更高版本不支持路由组，因此对这些集群显示空列。

- 故障转移组

  显示故障转移组的名称。

Qtrees 选项卡

Qtrees 选项卡显示有关 qtree 及其配额的详细信息。如果要编辑一个或多个 qtree 的 qtree 容量的健康阈值设置，可以单击 编辑阈值 按钮。

使用 导出 按钮创建一个包含所有受监控 qtrees 详细信息的逗号分隔值 (.csv) 文件。导出到 CSV 文件时，您可以选择为当前存储 VM、当前集群中的所有存储 VM 或数据中心内所有集群中的所有存储 VM 创建 qtrees 报告。导出的 CSV 文件中会显示一些其他 qtrees 字段。

- 状态

  显示 qtree 的当前状态。状态可以是 Critical（）、Error（）、Warning（）或 Normal（）。

  您可以将鼠标指针移动到状态图标上方来查看有关为 qtree 生成的一个或多个事件的详细信息。

  如果 qtree 的状态由单个事件确定，则可以查看事件名称、触发事件的时间和日期、将事件分配给的管理员的名称以及事件的原因等信息。您可以使用*查看详细信息*查看有关此事件的更多信息。

  如果 qtree 的状态由相同严重程度的多个事件确定，则显示前三个事件，其中包含事件名称、事件触发的时间和日期以及分配事件的管理员的名称等信息。您可以通过单击事件名称查看有关这些事件的更多详细信

息。您还可以使用 查看所有事件 来查看生成的事件列表。

> 一个 qtree 可以具有多个严重性相同或不同的事件。但是，系统将仅显示最高严重性。例如，如果 qtree 具有严重性为“错误”和“警告”的两个事件，则仅显示“错误”严重性。

- **Qtree**

  显示 qtree 的名称。

- 集群

  显示 qtree 所在集群的名称。仅显示在导出的 CSV 文件中。

- **Storage Virtual Machine**

  显示包含 qtree 的Storage Virtual Machine （SVM）名称。仅显示在导出的 CSV 文件中。

- 卷

  显示 qtree 所在卷的名称。

  可以将指针移动到卷名称上方来查看卷的详细信息。

- 配额集

  指示 qtree 的配额是启用还是禁用。

- 配额类型

  指定配额针对用户、用户组还是 qtree。仅显示在导出的 CSV 文件中。

- 用户或组

  显示用户或用户组的名称。每个用户和用户组将有多行。如果配额类型是 qtree 或者未设置配额，则该列为空。仅显示在导出的 CSV 文件中。

- 磁盘已用**%**

  显示已用磁盘空间的百分比。如果设置了磁盘硬限制，则此值基于磁盘硬限制。如果配额设置为无磁盘硬限制，则该值基于卷数据空间。如果未设置配额或 qtree 所属卷上的配额已关闭，则网格页面中将显示“不适用”，CSV 导出数据中的字段为空。

- 磁盘硬限制

  显示分配给 qtree 的最大磁盘空间量。当达到此限制时，Unified Manager 将生成一个严重事件，并且不允许进一步的磁盘写入。在以下情况下，该值将显示为 “Unlimited”：如果设置了配额但没有磁盘硬限制，如果未设置配额，或者 qtree 所属卷上的配额已关闭。

- 磁盘软限制

  显示在生成警告事件之前为 qtree 分配的磁盘空间量。在以下情况下，此值将显示为 “Unlimited”：如果设置了配额但没有磁盘软限制，如果未设置配额，或者 qtree 所属的卷已关闭配额。默认情况下，此列处于隐藏状态。

- 磁盘阈值

  显示磁盘空间上设置的阈值。在以下情况下，该值将显示为 “Unlimited”：如果设置了配额但没有磁盘阈值限制，如果未设置配额，或者 qtree 所属卷上的配额已关闭。默认情况下，此列处于隐藏状态。

- 文件已用 %

  显示 qtree 中使用的文件的百分比。如果设置了文件硬限制，则此值基于文件硬限制。如果设置的配额没有文件硬限制，则不显示任何值。如果未设置配额或 qtree 所属卷上的配额已关闭，则网格页面中将显示 “不适用”，CSV 导出数据中的字段为空。

- 文件硬限制

  显示 qtree 上允许的文件数的硬限制。在以下情况下，该值将显示为 “Unlimited”：如果设置的配额没有文件硬限制，如果未设置配额，或者 qtree 所属卷上的配额已关闭。

- 文件软限制

  显示 qtree 上允许的文件数的软限制。在以下情况下，该值将显示为 “Unlimited”：如果设置了配额但没有文件软限制，如果未设置配额，或者 qtree 所属的卷上的配额已关闭。默认情况下，此列是隐藏的。

用户和组配额选项卡

显示有关所选存储 VM 的用户和用户组配额的详细信息。您可以查看配额状态、用户或用户组的名称、对磁盘和文件设置的软限制和硬限制、磁盘空间量和使用的文件数以及磁盘阈值等信息。您还可以更改与用户或用户组关联的电子邮件地址。

- 编辑电子邮件地址命令按钮

  打开“编辑电子邮件地址”对话框，其中显示所选用户或用户组的当前电子邮件地址。您可以修改电子邮件地址。如果编辑电子邮件地址字段为空，则会使用默认规则为所选用户或用户组生成电子邮件地址。

  如果多个用户的配额相同，这些用户的名称将显示为逗号分隔值。此外，默认规则不用于生成电子邮件地址，因此，您必须为要发送的通知提供所需的电子邮件地址。

- 配置电子邮件规则命令按钮

  使您能够创建或修改规则，为存储 VM 上配置的用户或用户组配额生成电子邮件地址。当发生配额违规时，会向指定的电子邮件地址发送通知。

- 状态

  显示配额的当前状态。状态可以是 Critical （）、Warning （）或 Normal （）。

  可以将指针移动到状态图标上方来查看有关为配额生成的一个或多个事件的详细信息。

  如果配额的状态由单个事件确定，您可以查看事件名称、触发事件的时间和日期、被分配该事件的管理员名称以及事件原因等信息。您可以使用*查看详细信息*查看有关该事件的更多信息。

  如果配额的状态由相同严重程度的多个事件确定，则显示前三个事件，其中包含事件名称、触发事件的时间和日期以及分配事件的管理员的名称等信息。您可以通过单击事件名称查看有关这些事件的更多详细信息。您还可以使用*查看所有事件*来查看生成的事件列表。

一个配额可以具有多个严重性相同或不同的事件。但是，系统将仅显示最高严重性。例如，如果配额具有严重性为“错误”和“警告”的两个事件，则仅显示“错误”严重性。

- 用户或组

  显示用户或用户组的名称。如果多个用户的配额相同，这些用户的名称将显示为逗号分隔值。

  当 ONTAP 由于 SecD 错误而未提供有效的用户名时，该值将显示为 “Unknown”。

- 类型

  指定配额针对用户还是用户组。

- **Volume** 或 **Qtree**

  显示指定了用户或用户组配额的卷或 qtree 的名称。

  可以将指针移动到卷或 qtree 名称上方来查看卷或 qtree 的详细信息。

- 磁盘已用**%**

  显示已使用磁盘空间的百分比。如果配额设置为无磁盘硬限制，则该值显示为 “Not applicable”。

- 磁盘硬限制

  显示分配给配额的最大磁盘空间量。当达到此限制且不允许进一步的磁盘写入时，Unified Manager 会生成一个严重事件。如果配额设置为无磁盘硬限制，则该值显示为 “Unlimited”。

- 磁盘软限制

  显示在生成警告事件之前为配额分配的磁盘空间量。如果配额设置为无磁盘软限制，则该值显示为 “Unlimited”。默认情况下，此列是隐藏的。

- 磁盘阈值

  显示磁盘空间上设置的阈值。如果配额设置为无磁盘阈值限制，则该值显示为 “Unlimited”。默认情况下，此列处于隐藏状态。

- 文件已用 **%**

  显示 qtree 中使用的文件的百分比。如果配额设置为无文件硬限制，则该值显示为 “Not applicable”。

- 文件硬限制

  显示配额允许的文件数的硬限制。如果配额未设置文件硬限制，则该值显示为 “Unlimited”。

- 文件软限制

  显示配额上允许的文件数的软限制。如果配额设置为无文件软限制，则该值显示为 “Unlimited”。默认情况下，此列处于隐藏状态。

- 电子邮件地址

显示违反配额时将通知发送到的用户或用户组的电子邮件地址。

NFS 共享选项卡

“NFS 共享”选项卡显示有关 NFS 共享的信息，例如其状态、与卷（FlexGroup 卷或 FlexVol 卷）关联的路径、客户端对 NFS 共享的访问级别以及为导出的卷定义的导出策略。在以下情况下不会显示 NFS 共享：卷未挂载，或者与卷的导出策略关联的协议不包含 NFS 共享。

- 状态

  显示 NFS 共享的当前状态。状态可以是 Error （）或 Normal （）。

- 接合路径

  显示卷的挂载路径。如果将显式 NFS 导出策略应用到 qtree，则该列显示用于访问 qtree 的卷路径。

- 接合路径活动

  显示用于访问已挂载卷的路径处于活动状态还是非活动状态。

- **Volume** 或 **Qtree**

  显示 NFS 导出策略应用到的卷或 qtree 的名称。如果将 NFS 导出策略应用到卷中的 qtree，则该列显示卷和 qtree 的名称。

  您可以单击此链接，在相应的详细信息页面中查看对象的详细信息。如果对象是 qtree，将为 qtree 和卷显示链接。

- 卷状态

  显示要导出的卷的状况。该状况可以是“脱机”、“联机”、“受限”或“混合”。

  - 脱机

    不允许对卷进行读写访问。

  - 联机

    允许对卷进行读写访问。

  - 受限

    允许执行有限的操作（如奇偶校验重建），但不允许数据访问。

  - 混合

    FlexGroup 卷的成分卷并非都处于相同状况。

- 安全风格

  显示已导出卷的访问权限。安全模式可以是“UNIX”、“统一”、“NTFS”或“混合”。

  - UNIX（NFS 客户端）

卷中的文件和目录具有 UNIX 权限。

- 统一

  卷中的文件和目录具有统一安全模式。

- NTFS（CIFS 客户端）

  卷中的文件和目录具有 Windows NTFS 权限。

- 混合

  卷中的文件和目录可以具有 UNIX 权限或 Windows NTFS 权限。

- **UNIX** 权限

  以八进制字符串格式显示为已导出卷设置的 UNIX 权限位。这与 UNIX 模式权限位类似。

- 导出策略

  显示用于为已导出卷定义访问权限的规则。您可以单击链接查看有关与导出策略关联的规则的详细信息，例如身份验证协议和访问权限。

SMB Shares 选项卡

显示有关所选存储 VM 上的 SMB 共享的信息。您可以查看 SMB 共享的状态、共享名称、与存储 VM 关联的路径、共享的连接路径的状态、包含对象、包含卷的状态、共享的安全数据以及为共享定义的导出策略等信息。您还可以确定是否存在 SMB 共享的等效 NFS 路径。

文件夹中的共享未显示在“SMB 共享”选项卡中。

- 查看用户映射命令按钮

  启动“用户映射”对话框。

  您可以查看 storage VM 的用户映射详细信息。

- 显示 **ACL** 命令按钮

  为共享启动“访问控制”对话框。

  您可以查看选定共享的用户和权限详细信息。

- 状态

  显示共享的当前状态。状态可以是 Normal （ ） 或 Error （ ）。

- 共享名称

  显示 SMB 共享的名称。

- 路径

显示创建共享的接合路径。

- 接合路径活动

  显示用于访问共享的路径处于活动状态还是非活动状态。

- 包含对象

  显示共享所属父对象的名称。父对象可以是卷或 qtree。

  通过单击链接，您可以在相应的“详细信息”页面中查看有关包含对象的详细信息。如果包含对象是 qtree，则会同时显示 qtree 和 volume 的链接。

- 卷状态

  显示要导出的卷的状况。该状况可以是“脱机”、“联机”、“受限”或“混合”。

  - 脱机

    不允许对卷进行读写访问。

  - 联机

    允许对卷进行读写访问。

  - 受限

    允许执行有限的操作（如奇偶校验重建），但不允许数据访问。

  - 混合

    FlexGroup 卷的成分卷并非都处于相同状况。

- 安全

  显示已导出卷的访问权限。安全模式可以是“UNIX”、“统一”、“NTFS”或“混合”。

  - UNIX（NFS 客户端）

    卷中的文件和目录具有 UNIX 权限。

  - 统一

    卷中的文件和目录具有统一安全模式。

  - NTFS（CIFS 客户端）

    卷中的文件和目录具有 Windows NTFS 权限。

  - 混合

    卷中的文件和目录可以具有 UNIX 权限或 Windows NTFS 权限。

- 导出策略

  显示适用于共享的导出策略的名称。如果未为存储 VM 指定导出策略，则该值将显示为未启用。

  您可以单击此链接以查看与导出策略相关联的规则的详细信息，例如访问协议和权限。如果禁用了选定存储 VM 的导出策略，则该链接将被禁用。

- **NFS** 等效项

  指定共享是否存在 NFS 等效对象。

SAN 选项卡

显示选定存储 VM 的 LUN、启动器组和启动器的详细信息。默认情况下，将显示 LUN 视图。您可以在“启动器组”选项卡中查看有关启动器组的详细信息，并在“启动器”选项卡中查看有关启动器的详细信息。

- **LUN** 选项卡

  显示属于所选存储虚拟机的 LUN 的详细信息。您可以查看 LUN 名称、LUN 状态（联机或脱机）、包含 LUN 的文件系统（卷或 qtree）的名称、主机操作系统的类型、LUN 的总数据容量和序列号等信息。LUN 性能列提供了指向 LUN/性能详细信息页面的链接。

  您还可以查看有关是否在 LUN 上启用了精简配置以及该 LUN 是否映射到启动器组的信息。如果它已映射到启动器，您可以查看映射到选定 LUN 的启动器组和启动器。

- 启动程序组选项卡

  显示有关启动程序组的详细信息。您可以查看有关启动程序组的名称、访问状况、组中所有启动程序使用的主机操作系统类型以及支持的协议等详细信息。单击访问状况列中的链接时，您可以查看启动程序组的当前访问状况。

  - 正常

    启动程序组连接到多个访问路径。

  - 单条路径

    启动程序组连接到一个访问路径。

  - 无路径

    没有连接到启动程序组的访问路径。

    您可以查看启动程序组通过某个端口集映射到所有接口还是特定接口。单击“已映射接口”列中的计数链接将显示某个端口集的所有接口或特定接口。不会显示通过目标门户映射的接口。将显示映射到启动程序组的启动程序和 LUN 总数。

  此外，您还可以查看映射到选定启动程序组的 LUN 和启动程序。

- “启动器”选项卡

  显示启动器的名称和类型，以及映射到选定存储 VM 的此启动器的启动器组总数。

```
initiator groups that are mapped to the selected initiator group.
```

相关标注窗格

Related Annotations （相关批注）窗格用于查看与所选存储虚拟机关联的批注详细信息。详细信息包括应用于存储虚拟机的批注名称和批注值。您还可以从 Related Annotations （相关批注）窗格中删除手动批注。

相关设备窗格

Related Devices 窗格用于查看与存储 VM 相关的群集、聚合和卷：

- 集群

  显示 storage VM 所属集群的健康状态。

- 聚合

  显示属于所选存储 VM 的聚合数。还会根据最高严重性级别显示聚合的健康状态。例如，如果存储 VM 包含十个聚合，其中五个显示“警告”状态，其余五个显示“严重”状态，则显示的状态为“严重”。

- 分配的聚合

  显示分配给 storage VM 的聚合数。还会根据最高严重性级别显示聚合的健康状态。

- 卷

  显示属于所选存储虚拟机的卷的数量和容量。系统还会根据最高严重性级别显示卷的运行状况。当存储虚拟机中有 FlexGroup 卷时，计数还包括 FlexGroups；它不包括 FlexGroup 成分。

相关组窗格

使用“相关组”窗格，可以查看与所选存储 VM 关联的组列表。

相关警报窗格

Related Alerts（相关警报）窗格用于查看为选定存储 VM 创建的警报列表。您还可以通过单击 添加警报 链接添加警报，或通过单击警报名称编辑现有警报。

在 **Active IQ Unified Manager** 中查看集群/运行状况详细信息页面

集群/运行状况详细信息页面提供有关选定集群的详细信息，例如运行状况、容量和配置详细信息。您还可以查看有关集群的网络接口（LIF）、节点、磁盘、相关设备和相关警报的信息。

集群名称旁边的状态（例如“良好”）表示通信状态；Unified Manager 是否可以与集群通信。它不代表集群的故障转移状态或整体状态。

命令按钮

命令按钮可用于对选定集群执行以下任务：

- 切换到性能视图

  使您能够导航到“集群/性能详细信息”页面。

- 操作

  - 添加警报：打开“添加警报”对话框，通过该对话框可以将警报添加到选定集群。
  - 重新发现：启动集群的手动刷新，使 Unified Manager 能够发现集群的最新更改。

    如果 Unified Manager 与 OnCommand Workflow Automation 配对，则重新发现操作还会从 WFA（如果有）重新获取缓存数据。

  启动重新发现操作后，将显示指向相关作业详细信息的链接，以便跟踪作业状态。

  - 注释：使您能够对选定集群进行注释。

- 查看集群

  使您能够导航到“运行状况：所有群集”视图。

运行状况选项卡

显示有关各种集群对象（如节点、SVM 和聚合）的数据可用性和数据容量问题的详细信息。可用性问题与集群对象的数据服务能力有关。容量问题与集群对象的数据存储能力有关。

您可以单击对象的图形来查看对象的过滤列表。例如，您可以单击显示警告的 SVM 容量图来查看已筛选的 SVM 列表。此列表包含具有卷或 qtree 的 SVM，这些卷或 qtree 具有严重程度为“警告”的容量问题。您还可以单击显示警告的 SVM 可用性图表，以查看存在严重程度为“警告”的可用性问题的 SVM 列表。

可用性问题

以图形方式显示对象总数，包括存在可用性问题的对象和不存在任何可用性相关问题的对象。图中的颜色表示问题的不同严重程度。图表下方的信息提供了有关可能影响或已经影响集群中数据可用性的可用性问题的详细信息。例如，显示有关已关闭的磁盘架和离线的聚合的信息。

SFO 条形图显示的数据基于节点的 HA 状态。系统将根据生成的事件计算所有其他条形图显示的数据。

容量问题

以图形方式显示对象总数，包括存在容量问题的对象和不存在任何容量相关问题的对象。图中的颜色表示问题的不同严重程度。图表下方的信息提供了有关可能影响或已经影响集群中数据容量的容量问题的详细信息。例如，显示有关可能违反设定阈值的聚合的信息。

容量选项卡

显示有关选定集群容量的详细信息。

容量

显示所有分配聚合的已用容量和可用容量的数据容量图：

- 已用逻辑空间

  此集群上所有聚合中存储的数据的实际大小，未应用使用 ONTAP 存储效率技术所节省的空间。这不包括 Snapshot 副本。

- 数据缩减

  显示不包含 Snapshot 副本且保留两位有效数字的比率，例如 1.8 比 1。此比率基于配置的 ONTAP 存储效率设置。

- 已用

  所有聚合上的数据所使用的物理容量。这不包括用于奇偶校验、适当调整大小和预留的容量。

- 可用

  显示可用于数据的容量。

- 备用

  显示所有备用磁盘中可用于存储的可存储容量。

- 已配置

  显示为所有底层卷配置的容量。

详细信息

显示有关已用和可用容量的详细信息。计算不包括根聚合数据。

- 总容量

  显示集群的总容量。这不包括为奇偶校验分配的容量。

- 已用

  显示数据使用的容量。这不包括用于奇偶校验、规模调整和预留的容量。

- 可用

  显示可用于数据的容量。

- 已配置

  显示为所有底层卷配置的容量。

- 备用

  显示所有备用磁盘中可用于存储的可存储容量。

云层

显示已使用的云层总容量，以及集群上启用了 FabricPool 的聚合的每个已连接云层所使用的容量。FabricPool 可以是已获得许可的，也可以是未获得许可的。

物理容量细分 (按磁盘类型)

“按磁盘类型划分的物理容量”区域显示有关集群中各种类型磁盘的磁盘容量的详细信息。通过单击磁盘类型，您可以从“磁盘”选项卡中查看有关该磁盘类型的更多信息。

- 总可用容量

  显示数据磁盘的可用容量和备用容量。

- HDD

  以图形方式显示集群中所有 HDD 数据磁盘的使用容量和可用容量。虚线表示 HDD 中数据磁盘的备用容量。

- 闪存
  - SSD Data

    以图形方式显示集群中 SSD 数据磁盘的使用容量和可用容量。

  - SSD 缓存

    以图形方式显示集群中 SSD 缓存磁盘的可存储容量。

  - SSD 备用

    以图形方式显示集群中 SSD、数据和缓存磁盘的备用容量。

- 未分配磁盘

  显示集群中未分配磁盘的数量。

存在容量问题的聚合列表

以表格形式显示有关存在容量风险问题的聚合的已用容量和可用容量的详细信息。

- 状态

  表示聚合存在一定严重程度的容量相关问题。

  您可以将指针移到状态上，查看有关为聚合生成的事件的详细信息。

  如果聚合的状态由单个事件确定，则可以查看事件名称、触发事件的时间和日期、获分配该事件的管理员名称以及事件原因等信息。您可以单击*查看详细信息*按钮查看有关此事件的更多信息。

  如果聚合的状态由相同严重程度的多个事件确定，则会显示前三个事件，其中包含事件名称、触发事件的时间和日期以及事件所分配的管理员名称等信息。您可以通过单击事件名称查看有关每个事件的更多详细信息。您还可以单击 查看所有事件 链接以查看生成的事件列表。

聚合可以具有相同严重程度或不同严重程度的多个与容量相关的事件。但是，只会显示最高的严重程度。例如，如果聚合有两个事件，其严重程度级别为 Error 和 Critical，则仅显示 Critical 严重程度。

- 聚合

  显示聚合的名称。

- 已用数据容量

  以图形方式显示有关聚合容量使用情况的信息（百分比）。

- 达到全满前的天数

  显示聚合达到满载之前的预计剩余天数。

配置选项卡

显示有关选定集群的详细信息，例如 IP 地址、联系人和位置：

集群概述

- 管理接口

  显示 Unified Manager 用于连接集群的集群管理 LIF。还会显示该接口的运行状态。

- 主机名或 IP 地址

  显示 Unified Manager 用于连接集群的集群管理 LIF 的 FQDN、简称或 IP 地址。

- FQDN

  显示群集的完全限定域名（FQDN）。

- 操作系统版本

  显示集群正在运行的 ONTAP 版本。如果集群中的节点正在运行不同版本的 ONTAP，则会显示最早的 ONTAP 版本。

- 联系方式

  显示有关在集群出现问题时应联系的管理员的详细信息。

- 位置

  显示集群的位置。

- 个人设置

  标识这是否为全 SAN 阵列配置的集群。

远程集群概述

提供 MetroCluster 配置中远程集群的详细信息。此信息仅针对 MetroCluster 配置显示。

- 集群

  显示远程集群的名称。您可以单击集群名称以导航到集群的详细信息页面。

- 主机名或 IP 地址

  显示远程集群的 FQDN、短名称或 IP 地址。

- 位置

  显示远程集群的位置。

MetroCluster 概述

提供有关 MetroCluster over FC 或 MetroCluster over IP 配置中的本地集群的详细信息。此信息仅针对 MetroCluster over FC 或 IP 配置显示。

- 类型

  显示 MetroCluster 类型是双节点还是四节点。对于 MetroCluster over IP，仅支持四节点。

- 配置

  显示通过 FC 和 IP 的 MetroCluster 配置，可以具有以下值：

适用于 **FC**

- 使用 SAS 缆线的延伸型配置
- 使用 FC-SAS 网桥的延伸型配置
- 使用 FC 交换机的光纤配置

  对于四节点 MetroCluster，仅支持使用 FC 交换机的光纤配置。

用于 **IP**

- 使用以太网交换机进行 IP 配置（L2 或 L3，具体取决于集群的配置方式）
  - 自动计划外切换（AUSO）

    显示是否为本地群集启用了自动计划外切换。默认情况下，为 Unified Manager 中双节点 MetroCluster 配置中的所有群集启用 AUSO。您可以使用命令行界面更改 AUSO 设置。仅基于 FC 的 MetroCluster 支持此功能。

  - 切换模式

    显示基于 IP 的 MetroCluster 配置的切换模式。可用值为： `Active`、 `Negotiated Switchover` 和 `Automatic Unplanned Switchover`。

节点

- 可用性

  显示集群中 up（）或 down（）的节点数。

- 操作系统版本

  显示节点正在运行的 ONTAP 版本以及运行特定 ONTAP 版本的节点数量。例如，9.6 （2）、9.3 （1） 表示有两个节点运行 ONTAP 9.6，一个节点运行 ONTAP 9.3。

Storage Virtual Machines

- 可用性

  显示集群中已启动（）或已停止（）的 SVM 数量。

网络接口

- 可用性

  显示集群中 up（）或 down（）的非数据 LIF 的数量。

- 集群管理接口

  显示群集管理 LIF 的数量。

- 节点管理接口

  显示节点管理 LIF 的数量。

- 集群接口

  显示集群 LIF 的数量。

- 集群间接口

  显示集群间 LIF 的数量。

协议

- 数据协议

  显示为集群启用的许可数据协议的列表。数据协议包括 iSCSI、CIFS、NFS、NVMe 和 FC/FCoE。

数据保护

- 调解器

  显示集群是否支持介体以及介体的连接状态。它指示是否已配置介体，如果已配置，则显示介体的状态。

  - 不适用

在集群不支持介体时显示。

- 未配置

  在群集支持介体但未配置介体时显示。

- IP 地址

  当集群支持调解器且已配置调解器时显示。调解器状态由颜色指示。绿色表示调解器状态为可达。红色表示调解器状态为不可达。

云层

列出此集群连接到的云层的名称。它还列出了类型（Amazon S3、Microsoft Azure Cloud、IBM Cloud Object Storage、Google Cloud Storage、Alibaba Cloud Object Storage 或 StorageGRID）以及云层的状态（可用或不可用）。

MetroCluster 连接选项卡

显示 MetroCluster over FC 配置中集群组件的问题和连接状态。当集群的灾难恢复合作伙伴出现问题时，集群将显示在红色框中。

MetroCluster 连接选项卡仅对采用 MetroCluster over FC 配置的集群显示。

您可以通过单击远程集群的名称导航到远程集群的详细信息页面。您还可以通过单击组件的计数链接查看组件的详细信息。例如，单击集群中节点的计数链接会显示集群详细信息页面中的节点选项卡。单击远程集群中磁盘的计数链接会在远程集群的详细信息页面中显示磁盘选项卡。

管理八节点 MetroCluster 配置时，单击“磁盘架”组件的计数链接仅显示默认 HA 对的本地磁盘架。此外，无法显示另一个 HA 对上的本地磁盘架。

您可以将指针移到组件上，以便在出现任何问题时查看集群的详细信息和连接状态，并查看有关针对该问题生成的事件的更多信息。

如果组件之间的连接问题的状态由单个事件确定，则可以查看事件名称、触发事件的时间和日期、将事件分配给的管理员的名称以及事件的原因等信息。“查看详细信息”按钮提供有关事件的详细信息。

如果组件之间的连接问题的状态由相同严重程度的多个事件确定，则显示前三个事件，其中包含事件名称、触发事件的时间和日期以及事件分配给的管理员的名称等信息。您可以通过单击事件名称查看有关这些事件的更多详细信息。您还可以单击*查看所有事件*链接以查看生成的事件列表。

MetroCluster 复制选项卡

显示在基于 FC 的 MetroCluster 配置中正在复制的数据的状态。您可以使用“MetroCluster 复制”选项卡，通过与已对等集群同步镜像数据来确保数据保护。当集群的灾难恢复合作伙伴出现问题时，集群将显示在红色框中。

MetroCluster 复制选项卡仅对采用 MetroCluster over FC 配置的集群显示。

在 MetroCluster 环境中，您可以使用此选项卡验证本地集群与远程集群的逻辑连接和对等关系。您可以查看集群组件及其逻辑连接的客观表示。这有助于识别元数据和数据镜像过程中可能发生的问题。

在 MetroCluster 复制选项卡中，本地集群提供所选集群的详细图形表示，MetroCluster 合作伙伴是指远程集群。

网络接口选项卡

显示选定集群上创建的所有非数据 LIF 的详细信息。

网络接口

显示在选定集群上创建的 LIF 的名称。

运行状态

显示接口的运行状态，可以是 Up（）、Down（）或 Unknown（）。网络接口的运行状态取决于其物理端口的状态。

管理状态

显示接口的管理状态，可以是 Up（）、Down（）或 Unknown（）。您可以在更改配置时或在维护期间控制接口的管理状态。管理状态可以与操作状态不同。但是，如果 LIF 的管理状态为 Down，则默认情况下运行状态为 Down。

IP 地址

显示接口的 IP 地址。

角色

显示接口的角色。可能的角色是群集管理 LIF、节点管理 LIF、群集 LIF 和群集间 LIF。

主端口

显示最初与接口关联的物理端口。

当前端口

显示接口当前关联的物理端口。LIF 迁移后，当前端口可能与主端口不同。

故障转移策略

显示为接口配置的故障转移策略。

路由组

显示路由组的名称。可以单击路由组名称来查看有关路由和目标网关的详细信息。

ONTAP 8.3 或更高版本不支持路由组，因此对这些集群显示空列。

故障转移组

显示故障转移组的名称。

显示有关选定集群中节点的信息。您可以查看有关 HA 对、磁盘架和端口的详细信息：

HA 详细信息

提供 HA 对中节点的 HA 状态和健康状态的图示。节点的健康状态由以下颜色表示：

- 绿色

  节点处于工作状态。

- 黄色

  此节点已接管配对节点或此节点面临一些环境问题。

- 红色

  此节点已关闭。

您可以查看有关 HA 对可用性的信息，并采取必要的措施来防止任何风险。例如，在可能发生接管操作的情况下，将显示以下消息：可能发生存储故障转移。

您可以查看与 HA 对及其环境相关的事件列表，例如风扇、电源、NVRAM 电池、闪存卡、服务处理器和磁盘架连接。您还可以查看触发事件的时间。

您可以查看其他与节点相关的信息，例如型号。

如果存在单节点群集，还可以查看有关节点的详细信息。

磁盘架

显示有关 HA 对中磁盘盘架的信息。

您还可以查看为磁盘架和环境组件生成的事件，以及事件触发的时间。

- 磁盘架 **ID**

  显示磁盘所在的盘架的 ID。

- 组件状态

  显示磁盘架的环境详细信息，例如电源、风扇、温度传感器、电流传感器、磁盘连接和电压传感器。环境详细信息显示为以下颜色的图标：

  - 绿色

    环境组件工作正常。

  - 灰色

    没有可用于环境组件的数据。

- 红色

  某些环境组件已关闭。

- **State**

  显示磁盘架的状态。可能的状态为 Offline、Online、No status、Initialization required、Missing 和 Unknown。

- 型号

  显示磁盘架的型号。

- 本地磁盘架

  指示磁盘架是位于本地集群还是远程集群上。此列仅为 MetroCluster 配置中的集群显示。

- 唯一 **ID**

  显示磁盘架的唯一标识符。

- 固件版本

  显示磁盘架的固件版本。

端口

显示有关关联 FC、FCoE 和以太网端口的信息。您可以通过单击端口图标查看有关端口和相关 LIF 的详细信息。

您还可以查看为端口生成的事件。

您可以查看以下端口详细信息：

- 端口 ID

  显示端口的名称。例如，端口名称可以为 e0M、e0a 和 e0b。

- 角色

  显示端口的角色。可能的角色包括 Cluster、Data、Intercluster、Node-Management 和 Undefined。

- 类型

  显示用于端口的物理层协议。可能的类型有以太网、光纤通道和 FCoE。

- WWPN

  显示端口的全球通用端口名称（WWPN）。

- 固件修订版

  显示 FC/FCoE 端口的固件版本。

- 状态

  显示端口的当前状态。可能的状态为 Up、Down、Link Not Connected 或 Unknown（）。

  您可以从事件列表中查看与端口相关的事件。您还可以查看关联的 LIF 详细信息，例如 LIF 名称、运行状态、IP 地址或 WWPN、协议、与 LIF 关联的 SVM 的名称、当前端口、故障转移策略和故障转移组。

磁盘选项卡

显示选定集群中磁盘的详细信息。您可以查看与磁盘相关的信息，例如使用的磁盘数、备用磁盘数、损坏的磁盘数和未分配的磁盘数。您还可以查看其他详细信息，例如磁盘名称、磁盘类型和磁盘的所有者节点。

磁盘池摘要

显示按有效类型（FCAL、SAS、SATA、MSATA、SSD、NVMe SSD、SSD CAP、阵列 LUN 和 VMDISK）分类的磁盘数量以及磁盘的状态。您还可以查看其他详细信息，例如聚合、共享磁盘、备用磁盘、损坏的磁盘、未分配的磁盘和不受支持的磁盘的数量。如果单击有效磁盘类型计数链接，则会显示所选状态和有效类型的磁盘。例如，如果单击磁盘状态为 Broken 且有效类型为 SAS 的计数链接，则会显示磁盘状态为 Broken 且有效类型为 SAS 的所有磁盘。

磁盘

显示磁盘的名称。

RAID Groups

显示 RAID 组的名称。

所有者节点

显示磁盘所属节点的名称。如果磁盘未分配，则此列中不显示任何值。

州/省

显示磁盘的状态：聚合、共享、备用、损坏、未分配、不支持或未知。默认情况下，此列按以下顺序排列以显示状态：损坏、未分配、不支持、备用、聚合和共享。

本地磁盘

显示“是”或“否”以指示磁盘位于本地集群还是远程集群上。此列仅对 MetroCluster 配置中的集群显示。

位置

根据其容器类型显示磁盘的位置：例如，复制、数据或奇偶校验。默认情况下，此列处于隐藏状态。

受影响聚合

显示因磁盘故障而受影响的聚合数。您可以将指针悬停在计数链接上以查看受影响的聚合，然后单击聚合名称以查看聚合的详细信息。您还可以单击聚合计数，以在“运行状况：所有聚合”视图中查看受影响的聚合列表。

对于以下情况，此列中不显示任何值：

- 对于包含此类磁盘的群集添加到 Unified Manager 时损坏的磁盘
- 无故障磁盘时

存储池

显示 SSD 所属的存储池的名称。可以将指针移动到存储池名称上，以查看存储池的详细信息。

可存储容量

显示可用磁盘容量。

原始容量

显示在正确调整大小和 RAID 配置之前的原始未格式化磁盘的容量。默认情况下，此列处于隐藏状态。

类型

显示磁盘类型：例如 ATA、SATA、FCAL 或 VMDISK。

有效类型

显示由 ONTAP 分配的磁盘类型。

出于创建和添加到聚合以及备用管理的目的，某些 ONTAP 磁盘类型被认为是等效的。ONTAP 为每种磁盘类型分配有效的磁盘类型。

已用备用数据块 **%**

以百分比显示 SSD 磁盘中已消耗的备用块。对于 SSD 磁盘以外的磁盘，此列为空白。

已用额定寿命 **%**

根据实际 SSD 使用情况和制造商对 SSD 寿命的预测，以百分比形式显示已使用的 SSD 寿命估计值。值大于 99 表示估计的耐用度已耗尽，但可能并不表示 SSD 发生故障。如果该值未知，则忽略该磁盘。

固件

显示磁盘的固件版本。

RPM

显示磁盘的每分钟转数（RPM）。默认情况下，此列处于隐藏状态。

型号

显示磁盘的型号。默认情况下，此列处于隐藏状态。

供应商

显示磁盘供应商的名称。默认情况下，此列处于隐藏状态。

磁盘架 **ID**

显示磁盘所在的盘架的 ID。

托架

显示磁盘所在托架的 ID。

相关标注窗格

可让您查看与选定集群相关联的批注详细信息。详细信息包括应用于集群的批注名称和批注值。您还可以从“相关批注”窗格中删除手动批注。

相关设备窗格

使您能够查看与选定集群关联的设备详细信息。

详细信息包括连接到集群的设备的属性，例如设备类型、大小、数量和运行状况。您可以单击数量链接，对该特定设备进行进一步分析。

您可以使用 MetroCluster 合作伙伴窗格获取远程 MetroCluster 合作伙伴及其相关集群组件（如节点、聚合和 SVM）的计数和详细信息。仅为采用 MetroCluster 配置的集群显示 MetroCluster 合作伙伴窗格。

Related Devices 窗格用于查看和导航到与群集相关的节点、SVM 和聚合：

MetroCluster 配对集群

显示 MetroCluster 配对节点的健康状态。使用计数链接，您可以进一步导航并获取有关集群组件运行状况和容量的信息。

节点

显示属于选定集群的节点的数量、容量和健康状况。容量表示总可用容量与可用容量之比。

Storage Virtual Machines

显示属于选定集群的 SVM 数量。

聚合

显示属于选定集群的聚合的数量、容量和运行状况。

相关组窗格

使您能够查看包含选定集群的组列表。

相关警报窗格

“相关警报”窗格用于查看选定集群的警报列表。您还可以通过单击“添加警报”链接添加警报，或通过单击警报名称编辑现有警报。

相关信息

"卷页面" "查看集群列表和详细信息"

在 **Active IQ Unified Manager** 中查看聚合/运行状况详细信息页面

您可以使用“聚合/运行状况详细信息”页面查看有关所选聚合的详细信息，例如容量、磁盘信息、配置详细信息和生成的事件。您还可以查看有关该聚合的相关对象和相关警报的信息。

命令按钮

监控启用了 FabricPool 的聚合时，此页面上的已提交和超额提交值仅与本地（或性能层）容量相关。云层中的可用空间量未反映在超额提交值中。同样，聚合阈值仅与本地性能层相关。

通过命令按钮可以为选定的聚合执行以下任务：

- 切换到性能视图

  使您能够导航到“聚合/性能详细信息”页面。

- 操作
  - 添加警报

    使您能够向选定聚合添加警报。

  - 编辑阈值

    使您能够修改选定聚合的阈值设置。

- 查看聚合

  使您能够导航到“运行状况：所有聚合”视图。

容量选项卡

“容量”选项卡显示有关所选聚合的详细信息，例如其容量、阈值和每日增长率。

默认情况下，不会为根聚合生成容量事件。此外，Unified Manager 使用的阈值不适用于节点根聚合。只有技术支持代表可以修改要生成的这些事件的设置。当技术支持代表修改设置时，阈值将应用于节点根聚合。

- 容量

  显示数据容量图和 Snapshot 副本图，其中显示有关聚合的容量详细信息：

  - 已用逻辑空间

    在不应用 ONTAP 存储效率技术所节省的空间的情况下，存储在聚合上的数据的实际大小。

  - 已用

    聚合中数据使用的物理容量。

- 已过量提交

  当聚合中的空间超额配置时，图表将显示一个带有超额配置量的标志。

- 警告

  在设置警告阈值的位置显示虚线；这意味着聚合中的空间几乎已满。如果超出此阈值，则会生成“空间接近全满”事件。

- 错误

  在设置错误阈值的位置显示实线；这意味着聚合中的空间已满。如果超出此阈值，则会生成 Space Full 事件。

- Snapshot 副本图表

  只有已使用的 Snapshot 容量或 Snapshot 预留不为零时，才会显示此图形。

如果已用 Snapshot 容量超过 Snapshot 预留，这两个图表都会显示 Snapshot 容量超出 Snapshot 预留的容量。

- 云层

  显示启用了 FabricPool 的聚合在云层中数据所使用的空间。FabricPool 可以是已获得许可的，也可以是未获得许可的。

  当云层镜像到另一个云提供商（“**镜像层**”）时，此处将显示两个云层。

- 详细信息

  显示有关容量的详细信息。

  - 总容量

    显示聚合中的总容量。

  - 数据容量

    显示聚合使用的空间量（已用容量）和聚合中的可用空间量（可用容量）。

  - Snapshot 预留

    显示聚合的已用和可用 Snapshot 容量。

  - 已过量提交的容量

    显示聚合超额配置。只要当前未完全使用所有存储，聚合超额配置便可让您提供比给定聚合实际可用容量更多的存储。使用精简配置时，聚合中的卷总大小可能会超过聚合的总容量。

    如果对聚合进行了超额配置，则必须仔细监控其可用空间，并根据需要添加存储，以避免因空间不足而导致写入错误。

- 云层

  显示启用了 FabricPool 的聚合在云层中数据所使用的空间。FabricPool 可以是已获得许可的，也可以是未获得许可的。当云层镜像到另一个云提供商（镜像层）时，两个云层都会显示在此处

- 总缓存空间

  显示添加到 Flash Pool 聚合的固态驱动器（SSD）或分配单元的总空间。如果您已为聚合启用了 Flash Pool 但尚未添加任何 SSD，则缓存空间将显示为 0 KB。

  如果对聚合禁用了 Flash Pool，则此字段将隐藏。

- 聚合阈值

  显示以下聚合容量阈值：

  - 接近全满阈值

    指定聚合接近全满时的百分比。

  - 全满阈值

    指定聚合已满时的百分比。

  - 接近过量提交阈值

    指定聚合接近过量提交时的百分比。

  - 过量提交阈值

    指定聚合过量提交时的百分比。

- 其他详细信息：每日增长率

  如果最近两个样本之间的变化率持续 24 小时，则显示聚合中使用的磁盘空间。

  例如，如果聚合在下午 2 点使用 10 GB 磁盘空间，在下午 6 点使用 12 GB 磁盘空间，则此聚合的每日增长率（GB）为 2 GB。

- 卷移动

  显示当前正在进行的卷移动操作数：

  - 卷移出

    显示正在从聚合中移出的卷的数量和容量。

  您可以单击该链接以查看更多详细信息，例如卷名称、卷移动到的聚合、卷移动操作的状态以及估计的结束时间。

  - 卷移入

显示要移动到聚合中的卷的数量和剩余容量。

您可以单击该链接以查看更多详细信息，例如卷名称、从中移动卷的聚合、卷移动操作的状态以及估计的结束时间。

- Estimated used capacity after volume move

  显示卷移动操作完成后聚合中已用空间的估计量（以百分比表示，并以 KB、MB、GB 等为单位）。

- 容量概述 **-** 卷

  显示图形，提供有关聚合中所含卷容量的信息。系统将显示卷所用空间量（已用容量）以及卷中的可用空间量（可用容量）。当针对精简配置卷生成 Thin-Provisioned Volume Space At Risk 事件时，系统将显示卷所用空间量（已用容量）以及卷中可用但因聚合容量问题而无法使用的空间量（不可用容量）。

  您可以从下拉列表中选择要查看的图形。您可以对图形中显示的数据进行排序，以显示已用大小、已配置大小、可用容量、最快日增长率和最慢增长率等详细信息。您可以基于包含聚合中卷的存储虚拟机（SVM）筛选数据。您还可以查看精简配置卷的详细信息。您可以通过将光标定位在感兴趣的区域上来查看图形上特定点的详细信息。默认情况下，图形显示聚合中前 30 个筛选的卷。

磁盘信息选项卡

显示有关所选聚合中磁盘的详细信息，包括 RAID 类型和大小，以及聚合中使用的磁盘类型。该选项卡还以图形方式显示 RAID 组以及使用的磁盘类型（例如 SAS、ATA、FCAL、SSD 或 VMDISK）。通过将光标悬停在奇偶校验磁盘和数据磁盘上，您可以查看更多信息，例如磁盘的托架、磁盘架和转速。

- 数据

  以图形方式显示有关专用数据磁盘、共享数据磁盘或两者的详细信息。当数据磁盘包含共享磁盘时，将显示共享磁盘的图形详细信息。当数据磁盘包含专用磁盘和共享磁盘时，将显示专用数据磁盘和共享数据磁盘的图形详细信息。

  - **RAID** 详细信息

    仅显示专用磁盘的 RAID 详细信息。

    - 类型

      显示 RAID 类型（RAID0、RAID4、RAID-DP 或 RAID-TEC）。

    - 组大小

      显示 RAID 组中允许的最大磁盘数。

    - 组

      显示聚合中 RAID 组的数量。

  - 已用磁盘

    - 有效类型

      显示聚合中的数据磁盘类型（例如 ATA、SATA、FCAL、SSD 或 VMDISK）。

- 数据磁盘

  显示分配给聚合的数据磁盘的数量和容量。当聚合仅包含共享磁盘时，不显示数据磁盘详细信息。

- 奇偶校验磁盘

  显示分配给聚合的奇偶校验磁盘的数量和容量。当聚合仅包含共享磁盘时，不显示奇偶校验磁盘详细信息。

- 共享磁盘

  显示分配给聚合的共享数据磁盘的数量和容量。仅当聚合包含共享磁盘时，才会显示共享磁盘详细信息。

◦ 备用磁盘

显示选定聚合中可用于节点的备用数据磁盘的磁盘有效类型、数量和容量。

当聚合故障切换到配对节点时，Unified Manager 不会显示与该聚合兼容的所有备用磁盘。

- **SSD** 缓存

提供有关专用缓存 SSD 磁盘和共享缓存 SSD 磁盘的详细信息。

此时将显示专用缓存 SSD 磁盘的以下详细信息：

◦ **RAID** 详细信息

- 类型

  显示 RAID 类型（RAID0、RAID4、RAID-DP 或 RAID-TEC）。

- 组大小

  显示 RAID 组中允许的最大磁盘数。

- 组

  显示聚合中 RAID 组的数量。

◦ 已用磁盘

- 有效类型

  指示用于聚合中缓存的磁盘为 SSD 类型。

- 数据磁盘

  显示分配给聚合用于缓存的数据磁盘的数量和容量。

- 奇偶校验磁盘

  显示分配给聚合用于缓存的奇偶校验磁盘的数量和容量。

- 备用磁盘

  显示用于缓存的选定聚合中可用于节点的备用磁盘的磁盘有效类型、数量和容量。

  > 当聚合故障切换到配对节点时，Unified Manager 不会显示与该聚合兼容的所有备用磁盘。

  提供共享缓存的以下详细信息：

- 存储池

  显示存储池的名称。可以将指针移动到存储池名称上以查看以下详细信息：

  - 状态

    显示存储池的状态，可以是正常或不正常。

  - 总分配量

    显示存储池中的总分配单元和大小。

  - 分配单元大小

    显示存储池中可分配给聚合的最小空间量。

  - 磁盘

    显示用于创建存储池的磁盘数。如果存储池列中的磁盘数与该存储池的“磁盘信息”选项卡中显示的磁盘数不匹配，则表明一个或多个磁盘已损坏，并且存储池不正常。

  - 已用分配量

    显示聚合使用的分配单位的数量和大小。您可以单击聚合名称以查看聚合详细信息。

  - 可用分配量

    显示可用于节点的分配单元的数量和大小。您可以单击节点名称以查看聚合详细信息。

- 已分配缓存

  显示聚合使用的分配单位大小。

- 分配单元

  显示聚合使用的分配单位数。

- 磁盘

  显示存储池中包含的磁盘数。

- 详细信息

  - 存储池

显示存储池的数量。

- 总大小

  显示存储池的总大小。

- 云层

  如果已配置启用了 FabricPool 的聚合，则显示云层的名称，并显示已使用的总空间。当云层镜像到另一个云提供商（镜像层）时，此处将显示两个云层的详细信息

配置选项卡

“配置”选项卡会显示有关所选聚合的详细信息，例如其群集节点、块类型、RAID 类型、RAID 大小和 RAID 组计数：

- 概述
  - 节点

    显示包含所选聚合的节点的名称。

  - 数据块类型

    显示聚合的块格式：32 位或 64 位。

  - RAID 类型

    显示 RAID 类型（RAID0、RAID4、RAID-DP、RAID-TEC 或混合 RAID）。

  - RAID 大小

    显示 RAID 组的大小。

  - RAID Groups

    显示聚合中 RAID 组的数量。

  - SnapLock 类型

    显示聚合的 SnapLock 类型。

- 云层

  如果这是启用了 FabricPool 的聚合，则会显示云层的详细信息。某些字段因存储提供商而异。当云层镜像到另一个云提供商（“镜像层”）时，此处将显示两个云层。

  - 提供程序

    显示存储提供程序的名称，例如，StorageGRID、Amazon S3、IBM Cloud Object Storage、Microsoft Azure Cloud、Google Cloud Storage 或 Alibaba Cloud Object Storage。

  - 名称

显示 ONTAP 创建该云层时的名称。

- 服务器

  显示云层的 FQDN。

- 端口

  用于与云提供商通信的端口。

- 访问密钥或帐户

  显示此云层的访问密钥或帐户。

- 容器名称

  显示云层的存储分段或容器名称。

- SSL

  显示是否为此云层启用 SSL 加密。

历史记录区域

历史记录区域显示提供选定聚合容量信息的图形。此外，您可以点击*导出*按钮，以 CSV 格式为您正在查看的图表创建报告。

您可以从“历史记录”窗格顶端的下拉列表中选择图形类型。您也可以选择 1 周、1 个月或 1 年，查看特定时间段的详细信息。历史记录图表可以帮助您识别趋势：例如，如果聚合使用量始终超过几乎已满阈值，您可以采取适当的措施。

历史记录图显示下列信息：

- 已用聚合容量 **(%)**

  根据使用历史记录以折线图的形式在垂直（y）轴上以百分比形式显示聚合中的已用容量以及聚合容量使用趋势。时间段显示在水平（x）轴上。您可以选择一周、一个月或一年的时间段。您可以通过将光标定位在特定区域上来查看图形上特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，当您单击“已使用的容量”图例时，“已使用的容量”图形线条将被隐藏。

- 已用聚合容量与总容量

  根据使用历史记录以及已用容量和总容量（以字节、千字节、兆字节等为单位）在垂直（y）轴上以折线图形式显示聚合容量使用方式的趋势。时间段显示在水平（x）轴上。您可以选择一周、一个月或一年的时间段。您可以通过将光标放置在特定区域上来查看图形上特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，当您单击 Trend Capacity Used 图例时，Trend Capacity Used 图形线将被隐藏。

- 聚合已用容量（**%**）与已提交容量（**%**）

  根据使用历史记录显示聚合容量使用方式的趋势，以及在垂直（y）轴上以折线图形式按百分比显示已承诺空间。时间段显示在水平（x）轴上。您可以选择一周、一个月或一年的时间段。您可以通过将光标放置在特定区域上来查看图形上特定点的详细信息。您可以通过单击相应的图例来隐藏或显示折线图。例如，当您单击“已承诺空间”图例时，“已承诺空间”图形线条将被隐藏。

事件列表

“事件”列表显示有关新事件和已确认事件的详细信息：

- 严重程度

  显示事件的严重级别。

- 事件

  显示事件名称。

- 触发时间

  显示事件生成后经过的时间。如果经过的时间超过一周，则会显示生成事件的时间戳。

相关设备窗格

Related Devices 窗格可用于查看与聚合相关的集群节点、卷和磁盘：

- 节点

  显示包含聚合的节点的容量和运行状况。容量表示总可用容量与可用容量的比值。

- 节点中的聚合

  显示包含所选聚合的集群节点中所有聚合的数量和容量。还会根据最高严重性级别显示聚合的健康状态。例如，如果集群节点包含十个聚合，其中五个显示“警告”状态，其余五个显示“严重”状态，则显示的状态为“严重”。

- 卷

  显示聚合中 FlexVol 卷和 FlexGroup 卷的数量和容量；该数量不包括 FlexGroup 成分卷。还会根据最高严重性级别显示卷的运行状况。

- 资源池

  显示与聚合相关的资源池。

- 磁盘

  显示选定聚合中的磁盘数。

相关警报窗格

“相关警报”窗格用于查看为选定聚合创建的警报列表。您还可以通过单击添加警报链接添加警报，或通过单击警报名称编辑现有警报。

相关信息

"查看存储池详细信息"

保护和还原数据

创建保护关系并进行故障排除

Active IQ Unified Manager 中的 SnapMirror 保护类型

根据数据存储拓扑的部署，Unified Manager 允许您配置多种类型的 SnapMirror 保护关系。所有 SnapMirror 保护变体都提供故障转移灾难恢复保护，但在性能、版本灵活性和多备份副本保护方面提供不同的功能。

传统 SnapMirror 异步保护关系

传统的 SnapMirror 异步保护在源卷和目标卷之间提供块复制镜像保护。

在传统 SnapMirror 关系中，镜像操作比在替代 SnapMirror 关系中执行得更快，因为镜像操作基于块复制。但是，传统 SnapMirror 保护要求目标卷运行的 ONTAP 软件次要版本与源卷相同或更高（在同一主要版本内，例如，版本 8.x 到 8.x，或 9.x 到 9.x）。不支持从 9.1 源复制到 9.0 目标，因为目标运行的是较早的主要版本。

利用版本灵活的复制实现 SnapMirror 异步保护

具有版本灵活复制功能的 SnapMirror 异步保护可在源卷和目标卷之间提供逻辑复制镜像保护，即使这些卷运行在不同版本的 ONTAP 8.3 或更高版本软件下（例如，版本 8.3 到 8.3.1，或 8.3 到 9.1，或 9.2.2 到 9.2）。

在采用版本灵活复制的 SnapMirror 关系中，镜像操作不会像在传统 SnapMirror 关系中那样快速执行。

由于执行速度较慢，SnapMirror 具有版本灵活性的复制保护不适合在以下任一情况下实施：

- 源对象包含超过 1000 万个要保护的文件。
- 受保护数据的恢复点目标为两个小时或更短时间。（也就是说，目标必须始终包含比源数据早不超过两个小时的镜像可恢复数据。）

在列出的任一情况下，都需要执行速度更快的、基于块复制的默认 SnapMirror 保护。

SnapMirror 异步保护，具有版本灵活的复制和备份选项

SnapMirror 具有版本灵活的复制和备份选项的异步保护可在源卷和目标卷之间提供镜像保护，并能够在目标位置存储镜像数据的多个副本。

存储管理员可以指定将哪些 Snapshot 副本从源镜像到目标，还可以指定在目标处保留这些副本的时间，即使这些副本在源处被删除。

在具有版本灵活的复制和备份选项的 SnapMirror 关系中，镜像操作不会像在传统 SnapMirror 关系中那样快速执行。

SnapMirror 统一复制（镜像和保管库）

SnapMirror 统一复制允许您在同一目标卷上配置灾难恢复和归档。与 SnapMirror 一样，统一数据保护会在首次调用时执行基线传输。在默认统一数据保护策略 “MirrorAndVault” 下进行的基线传输会创建源卷的 Snapshot 副本，然后将该副本及其引用的数据块传输到目标卷。与 SnapVault 一样，统一数据保护不会在基线中包含较旧的

Snapshot 副本。

具有严格同步的 **SnapMirror** 同步保护

采用 “strict” 同步的 SnapMirror 同步保护可确保主卷和辅助卷始终是彼此的真实副本。如果在尝试将数据写入辅助卷时发生复制故障，则主卷的客户端 I/O 会中断。

具有常规同步的 **SnapMirror** 同步保护

SnapMirror 同步保护（采用 “regular” 同步）不需要主卷和辅助卷始终是彼此的真实副本；从而确保主卷的可用性。如果在尝试将数据写入辅助卷时发生复制失败，则主卷和辅助卷将不同步，并且客户端 I/O 将继续写入主卷。

从运行状况：所有卷视图或卷/运行状况详细信息页面监视同步保护关系时，还原按钮和关系操作按钮不可用。

SnapMirror 活动同步

SnapMirror 主动同步功能适用于 ONTAP 9.8 及更高版本，您可以使用它来保护具有 LUN 的应用程序，使应用程序能够透明地进行故障切换，从而在发生灾难时确保业务连续性。

它允许您从 Unified Manager 发现和监控群集和存储虚拟机上可用的一致性组（CG）的同步 SnapMirror 关系。SnapMirror 活动同步在 AFF 群集或全 SAN 阵列（ASA）群集上受支持，其中主群集和辅助群集可以是 AFF 或 ASA。SnapMirror 活动同步可保护具有 iSCSI 或 FCP LUN 的应用程序。

当您查看受 SnapMirror 活动同步关系保护的卷和 LUN 时，您可以获得保护关系的统一视图、卷清单中的一致性组、查看一致性组关系的保护拓扑、查看最多一年的一致性组关系的历史数据。您也可以下载报告。您还可以查看一致性组关系的摘要，支持搜索一致性组关系，并获取有关受一致性组保护的卷的信息。

在“关系”页面上，您还可以对受一致性组保护的源和目标存储对象及其关系进行排序、筛选和扩展保护。

要了解有关 SnapMirror 活动同步的更多信息，请参阅 "ONTAP 9 Snapmirror 活动同步文档（以前称为 SM-BC）"。

在 **Unified Manager** 中设置保护关系

在 **Active IQ Unified Manager** 中设置保护关系

要使用 Unified Manager 和 OnCommand Workflow Automation 设置 SnapMirror 和 SnapVault 关系来保护您的数据，必须执行几个步骤。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 必须在两个集群或两个存储虚拟机（SVMs）之间建立对等关系。
- 必须将 OnCommand Workflow Automation 与 Unified Manager 集成：
  - "设置 OnCommand Workflow Automation"。
  - "在 Workflow Automation 中验证 Unified Manager 数据源缓存"。

步骤

1. 根据您想要创建的保护关系类型，执行以下操作之一：
   - "创建 SnapMirror 保护关系"。
   - "创建 SnapVault 保护关系"。
2. 如果要为关系创建策略，请根据所创建的关系类型执行以下操作之一：
   - "创建 SnapVault 策略"。
   - "创建 SnapMirror 策略"。
3. "创建 SnapMirror 或 SnapVault 计划"。

配置 **Workflow Automation** 和 **Active IQ Unified Manager** 之间的连接

您可以配置 OnCommand Workflow Automation (WFA) 和 Unified Manager 之间的安全连接。通过连接到 Workflow Automation，您可以使用 SnapMirror 和 SnapVault 配置工作流等保护功能，以及管理 SnapMirror 关系的命令。

开始之前

- Workflow Automation 的安装版本必须为 5.1.1P6 或更高版本。

  "用于管理 Clustered Data ONTAP 的 WFA pack"包含在 WFA 5.1.1P6 中，因此无需像过去要求的那样从 NetAppStorage Automation Store 下载此包并将其单独安装到 WFA 服务器上。"WFA 下载"

- 您必须具有在 Unified Manager 中创建的数据库用户的名称，以支持 WFA 和 Unified Manager 连接。

  此数据库用户必须已被分配集成架构用户角色。

- 必须在 Workflow Automation 中为您分配 Administrator 角色或 Architect 角色。
- 要进行 Workflow Automation 设置，您必须具有主机地址、端口号 443、用户名和密码。
- 您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*常规* > **Workflow Automation**。
2. 在 *Workflow Automation 页面*的*数据库用户*区域中，选择名称，然后输入您为支持 Unified Manager 和 Workflow Automation 连接而创建的数据库用户的密码。
3. 在页面的 **Workflow Automation Credentials** 区域中，输入主机名或 IP 地址（IPv4 或 IPv6），以及 Workflow Automation 设置的用户名和密码。

   您必须使用 Unified Manager 服务器端口（端口 443）。

4. 单击 **Save**。
5. 如果使用自签名证书，请单击*是*以授权安全证书。

   此时将显示 Workflow Automation 页面。

6. 单击 是 重新加载 Web UI，并添加 Workflow Automation 功能。

相关信息

"NetApp 文档：OnCommand Workflow Automation（当前版本）"

在 **Workflow Automation** 中验证 **Active IQ Unified Manager** 数据源缓存

您可以通过在 Workflow Automation 中检查数据源采集是否成功来确定 Unified Manager 数据源缓存是否正常工作。在将 Workflow Automation 与 Unified Manager 集成以确保集成后 Workflow Automation 功能可用时，您可以执行此操作。

开始之前

要执行此任务，必须在 Workflow Automation 中为您分配管理员角色或架构师角色。

步骤

1. 从 Workflow Automation UI 中，选择 **Execution** > **Data Sources**。
2. 右键单击 Unified Manager 数据源的名称，然后选择*立即获取*。
3. 验证采集成功且没有错误。

   必须解决采集错误，Workflow Automation 才能与 Unified Manager 成功集成。

重新安装或升级 **OnCommand Workflow Automation** 如何影响 **Active IQ Unified Manager**

在重新安装或升级 OnCommand Workflow Automation 之前，您必须首先删除 OnCommand Workflow Automation 和 Unified Manager 之间的连接，并确保停止当前正在运行或计划的所有 OnCommand Workflow Automation 作业。

您还必须从 OnCommand Workflow Automation 手动删除 Unified Manager。

重新安装或升级 OnCommand Workflow Automation 后，必须再次设置与 Unified Manager 的连接。

从 **Active IQ Unified Manager** 中删除 **OnCommand Workflow Automation** 设置

当您不再希望使用 Workflow Automation 时，可以从 Unified Manager 中删除 OnCommand Workflow Automation 设置。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击左侧设置菜单中的*常规* > **Workflow Automation**。
2. 在 **Workflow Automation** 页面中，单击 **Remove Setup**。

执行保护关系故障转移和故障恢复

在 **Active IQ Unified Manager** 中执行保护关系故障转移和故障恢复

当保护关系中的源卷因硬件故障或灾难而被禁用时，您可以使用 Unified Manager 中的保

护关系功能使保护目标可读取/写入并故障切换到该卷，直到源再次联机；然后，当原始源可用于提供数据时，您可以故障回切到原始源。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 要执行此操作，您必须已设置 OnCommand Workflow Automation。

步骤

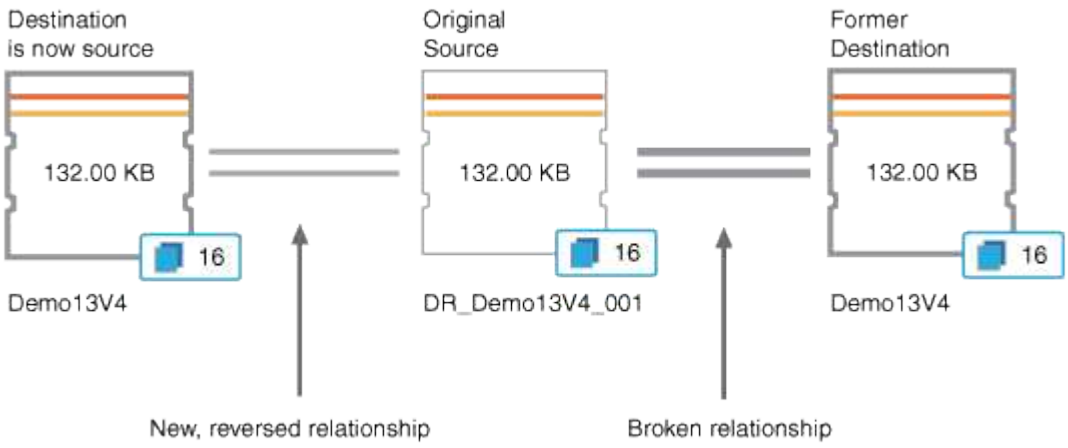
1. "断开 SnapMirror 关系"。

   必须先断开关系，然后才能将目标从数据保护卷转换为读/写卷，然后才能逆转关系。

2. "反转保护关系"。

   当原始源卷再次可用时，您可以决定通过恢复源卷来重新建立原始保护关系。在恢复源之前，必须将其与写入前一个目标的数据同步。您可以使用反向重新同步操作通过反转原始关系的角色并将源卷与以前的目标同步来创建新的保护关系。将为新关系创建新的基线 Snapshot 副本。

   反向关系看起来类似于级联关系：



3. "中断反向 SnapMirror 关系"。

   当原始源卷重新同步并可再次提供数据时，请使用 break 操作断开反向关系。

4. "删除此关系"。

   当不再需要反向关系时，您应该在重新建立原始关系之前删除该关系。

5. "重新同步关系"。

   使用重新同步操作将数据从源同步到目标，并重新建立原始关系。

从 **Active IQ Unified Manager** 卷/运行状况页面中断 **SnapMirror** 保护关系

您可以从卷/运行状况详细信息页面中断保护关系，并停止 SnapMirror 关系中源卷和目标卷之间的数据传输。当您要迁移数据、进行灾难恢复或应用程序测试时，可能会中断关

系。目标卷将更改为读写卷。您无法中断 SnapVault 关系。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

步骤

1. 在 卷/运行状况 详细信息页面的 保护 选项卡中，从拓扑中选择您要中断的 SnapMirror 关系。
2. 右键单击目标并从菜单中选择*断开*。

   此时将显示断开关系对话框。

3. 单击*继续*以中断此关系。
4. 在拓扑中，确认关系已中断。

从 **Active IQ Unified Manager** 中的卷/运行状况详细信息页面反转保护关系

当灾难导致保护关系中的源卷不可用时，您可以在修复或更换源卷期间将目标卷转换为读/写状态，从而使用目标卷来提供数据。当源再次可用于接收数据时，您可以使用反向重新同步操作建立反向关系，将源上的数据与读/写目标上的数据同步。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。
- 此关系不得为 SnapVault 关系。
- 保护关系必须已存在。
- 必须中断保护关系。
- 源和目标必须处于联机状态。
- 源不能是其他数据保护卷的目标。
- 执行此任务时，源上比通用 Snapshot 副本上的数据更新的数据将被删除。
- 在反向重新同步关系上创建的策略和计划与在原始保护关系上创建的策略和计划相同。

  如果策略和计划不存在，则会创建这些策略和计划。

步骤

1. 从*卷/运行状况*详细信息页面的*保护*选项卡中，在拓扑中找到要反转源和目标的 SnapMirror 关系，然后右键单击它。
2. 从菜单中选择*反向重新同步*。

   此时将显示反向重新同步对话框。

3. 验证*反向重新同步*对话框中显示的关系是否是要执行反向重新同步操作的关系，然后单击*提交*。

   反向重新同步对话框已关闭，作业链接显示在卷/运行状况详细信息页面的顶部。

4. *可选：*单击*卷/运行状况*详细信息页面上的*查看作业*以跟踪每个反向重新同步作业的状态。

   此时将显示已筛选的作业列表。

5. *可选：*单击浏览器上的*后退*箭头返回*卷/运行状况*详细信息页面。

   当所有作业任务成功完成时，反向重新同步操作完成。

从 **Active IQ Unified Manager** 的卷/运行状况详细信息页面中删除保护关系

您可以删除保护关系，以永久删除所选源和目标之间的现有关系：例如，当您希望使用其他目标创建关系时。此操作将删除所有元数据，并且无法撤消。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

步骤

1. 在*卷/健康*详细信息页面的*保护*选项卡中，从拓扑中选择要删除的 SnapMirror 关系。
2. 右键单击目标的名称，然后从菜单中选择*删除*。

   此时将显示删除关系对话框。

3. 单击*继续*删除此关系。

   将从 Volume / Health 详细信息页面中删除此关系。

从 **Active IQ Unified Manager** 中的卷/运行状况详细信息页面重新同步保护关系

您可以重新同步已中断且目标已变为读/写的 SnapMirror 或 SnapVault 关系上的数据，以便源上的数据与目标上的数据相匹配。当源卷上所需的通用 Snapshot 副本被删除，导致 SnapMirror 或 SnapVault 更新失败时，您也可以重新同步。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 OnCommand Workflow Automation。

步骤

1. 从*卷/运行状况*详细信息页面的*保护*选项卡中，在拓扑中找到要重新同步的保护关系，然后右键单击它。
2. 从菜单中选择*重新同步*。

   或者，从*操作*菜单中，选择*关系* > *重新同步*以重新同步您当前查看详细信息的关系。

   此时将显示重新同步对话框。

3. 在*重新同步选项*选项卡中，选择传输优先级和最大传输速率。
4. 单击*源 Snapshot 副本*；然后，在*Snapshot 副本*列中，单击*默认*。

此时将显示选择源 Snapshot 副本对话框。

5. 如果要指定现有 Snapshot 副本而不是传输默认 Snapshot 副本，请单击 现有 **Snapshot** 副本 并从列表中选择 Snapshot 副本。
6. 单击*提交*。

   此时将返回到“重新同步”对话框。

7. 如果选择了多个要重新同步的源，请单击要指定现有 Snapshot 副本的下一个源的 默认值。
8. 单击*提交*以开始重新同步作业。

   重新同步作业已启动，您将返回到卷/运行状况详细信息页面，并在页面顶部显示作业链接。

9. 可选： 单击 卷 / 运行状况详细信息 页面上的 查看作业 以跟踪每个重新同步作业的状态。

   此时将显示已筛选的作业列表。

10. *可选：*单击浏览器上的*后退*箭头返回*卷/运行状况*详细信息页面。

    当所有作业任务成功完成时，重新同步作业完成。

解决保护作业失败

解决 **Active IQ Unified Manager** 中的保护作业故障

此工作流程提供了如何从 Unified Manager 仪表板识别和解决保护作业失败的示例。

开始之前

由于此工作流中的某些任务要求您使用管理员角色登录，因此您必须熟悉使用各种功能所需的角色。

在这种情况下，您可以访问仪表板页面，查看保护作业是否存在任何问题。在“保护事件”区域，您注意到卷上出现“作业终止”事件，显示“保护作业失败”错误。您调查此错误以确定可能的原因和潜在的解决方案。

步骤

1. 在“仪表板未解决的事件和风险”区域的“保护事件”面板中，单击 保护作业失败 事件。

   事件的链接文本以 `object_name:/object_name - Error Name`的形式编写，例如 `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`。

   将显示失败的保护作业的事件详细信息页面。

2. 查看*摘要*区域的“原因”字段中的错误消息，以确定问题并评估潜在的纠正措施。

   请参阅 "识别问题并对失败的保护作业执行纠正措施"。

识别问题并在 **Active IQ Unified Manager** 中对失败的保护作业执行纠正措施

您可以在“事件详细信息”页面的“原因”字段中查看作业失败错误消息，并确定作业因 Snapshot 副本错误而失败。然后，您进入“卷 / 运行状况”详细信息页面以收集更多信息。

开始之前

您必须具有应用程序管理员角色。

“事件详细信息”页面的“原因”字段中提供的错误消息包含有关失败作业的以下文本：

```
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
```

此消息提供以下信息：

- 备份或镜像作业未成功完成。

  该作业涉及虚拟服务器 `cluster2_src_svm`上的源卷 `cluster2_src_vol2`与名为 `cluster3_dst_svm`的虚拟服务器上的目标卷 `managed_svc2_vol3`之间的保护关系。

- 源卷 `cluster2_src_svm:/cluster2_src_vol2`上 `0426cluster2_src_vol2snap`的 Snapshot 副本作业失败。

在这种情况下，您可以确定作业失败的原因和潜在的纠正措施。但是，解决故障需要访问 System Manager web UI 或 ONTAP CLI 命令。

步骤

1. 您查看错误消息并确定源卷上的 Snapshot 复制作业失败，这表明您的源卷可能存在问题。

   或者，您可以单击错误消息末尾的*作业详细信息*链接，但出于此场景的目的，您选择不执行此操作。

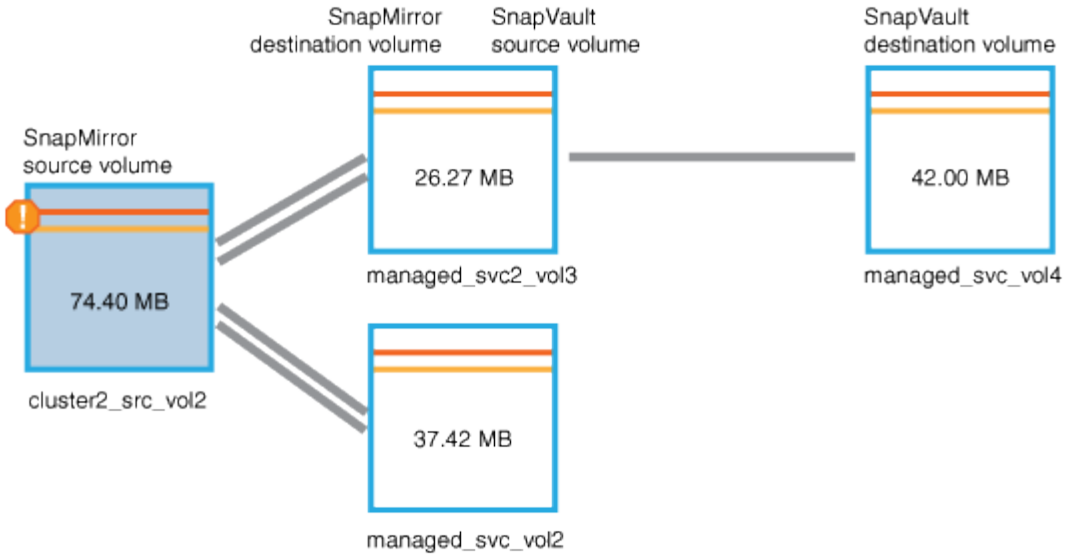
2. 您决定要尝试解决此事件，因此请执行以下操作：
   a. 单击*分配给*按钮，然后从菜单中选择*我*。
   b. 如果已为该事件设置了警报，请单击*确认*按钮，这样您就不会继续收到重复的警报通知。
   c. （可选）您也可以添加有关事件的备注。
3. 单击*摘要*窗格中的*源*字段可查看源卷的详细信息。

   源 字段包含源对象的名称：在本例中，即为计划了 Snapshot 副本作业的卷。

   此时将显示 `cluster2_src_vol2` 的“卷/运行状况”详细信息页面，其中显示“保护”选项卡的内容。

4. 查看保护拓扑图，您会看到一个与拓扑中的第一个卷相关联的错误图标，该卷是 SnapMirror 关系的源卷。

   您还可以在源卷图标中看到水平条，指示为该卷设置的警告和错误阈值。



5. 将光标悬停在错误图标上以查看显示阈值设置的弹出对话框，您会看到卷已超出错误阈值，这表明存在容量问题。
6. 单击 **Capacity** 选项卡。

   显示有关卷 `cluster2_src_vol2`的容量信息。

7. 在*容量*面板中，您会看到条形图中有一个错误图标，再次表明卷容量已超过为卷设置的阈值水平。
8. 在容量图表下方，您会看到已禁用卷自动增长并设置了卷空间保证。

   您可以决定启用自动增长，但出于本场景的目的，您决定在做出如何解决容量问题的决定之前进行进一步调查。

9. 您向下滚动到*事件*列表，看到生成了保护作业失败、卷达到全满前的天数和卷空间全满事件。
10. 在*事件*列表中，您单击*卷空间已满*事件以获取更多信息，因为您已确定此事件似乎与您的容量问题最相关。

    “事件详细信息”页面显示源卷的“卷空间已满”事件。

11. 在 摘要 区域中，您查看事件的原因字段： `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used`。
12. 在“摘要”区域下方，可以看到“建议的纠正措施”。

    “建议的纠正措施”仅针对某些事件显示，因此不会针对所有类型的事件显示此区域。

    您单击可执行的建议操作列表，以解决“卷空间已满”事件：

    - 对此卷启用自动增长。
    - 调整卷大小。
    - 对此卷启用并运行重复数据删除。
    - 对此卷启用并运行压缩。

13. 您决定在卷上启用自动增长，但为此，您必须确定父聚合上的可用空间和当前卷增长率：

a. 请查看 相关设备 窗格中的父聚合 `cluster2_src_aggr1`。

   您可以单击聚合的名称，以获取有关聚合的更多详细信息。

   您确定聚合有足够的空间来启用卷自动增长。

b. 在页面顶端，查看指示重大事件的图标，并查看图标下方的文本。

   您确定“剩余天数：不到一天 | 每日增长率：5.4%”。

14. 请转到 System Manager 或访问 ONTAP CLI 以启用该 `volume autogrow` 选项。

    记下卷和聚合的名称，以便在启用自动增长时可以使用它们。

15. 解决容量问题后，返回 Unified Manager **Event** 详细信息页面并将该事件标记为已解决。

解决 **Active IQ Unified Manager** 中的滞后问题

此工作流程提供了如何解决滞后问题的示例。在此场景中，您是一名管理员或操作员，正在访问 Unified ManagerDashboard 页面，以查看保护关系是否存在任何问题，如果存在，则寻找解决方案。

开始之前

您必须具有应用程序管理员或存储管理员角色。

在“控制面板”页面中，您可以查看“未解决的事件和风险”区域，并在“保护风险”下的“保护”窗格中看到“SnapMirror 滞后”错误。

步骤

1. 在*仪表板*页面的*保护*窗格中，找到 SnapMirror 关系延迟错误并单击它。

   此时将显示延迟错误事件的“事件详细信息”页面。

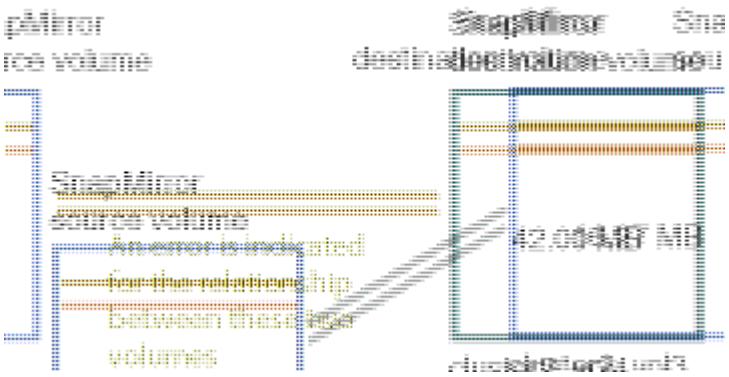
2. 从*事件*详细信息页面，您可以执行以下一项或多项任务：
   - 查看“摘要”区域的“原因”字段中的错误消息，以确定是否有任何建议的纠正措施。
   - 单击摘要区域的源字段中的对象名称（在本例中为卷），以获取有关该卷的详细信息。
   - 查找可能已添加的有关此事件的备注。
   - 为事件添加备注。
   - 将事件分配给特定用户。
   - 确认或解决此事件。

3. 在此场景中，您单击 **Summary** 区域 Source 字段中的对象名称（在本例中为卷），以获取有关该卷的详细信息。

   此时将显示“卷/健康详细信息”页面的“保护”选项卡。

4. 在*保护*选项卡中，您可以查看拓扑图。

您会注意到，带有滞后错误的卷是三卷 SnapMirror 级联中的最后一个卷。您选择的卷以深灰色轮廓显示，来自源卷的双橙色线条表示 SnapMirror 关系错误。



5. 单击 SnapMirror 级联中的每个卷。

   选择每个卷时，“摘要”、“拓扑”、“历史记录”、“事件”、“相关设备”和“相关警报”区域中的保护信息将更改为显示与所选卷相关的详细信息。

6. 您查看*摘要*区域，并将光标悬停在每个卷的*更新时间表*字段中的信息图标上。

   在这种情况下，您会注意到 SnapMirror 策略是 DPDefault，并且 SnapMirror 计划在每小时过 5 分钟时更新一次。您意识到关系中的所有卷都试图同时完成 SnapMirror 传输。

7. 要解决延迟问题，请修改两个级联卷的计划，以便每个目标在其源完成传输后开始 SnapMirror 传输。

管理和监控保护关系

了解如何在 **Active IQ Unified Manager** 中管理和监控保护关系

Active IQ Unified Manager 使您能够创建保护关系，监控托管集群上的 SnapMirror 和 SnapVault 关系并对其进行故障排除，并在数据被覆盖或丢失时还原数据。

对于 SnapMirror 操作，有两种复制类型：

- 异步

  从主卷到二级卷的复制由计划决定。

- 同步

  在主卷和二级卷上同时执行复制。

您最多可以同时执行 10 个保护作业，而不会影响性能。当您同时运行 11 到 30 个作业时，可能会遇到一些性能影响。不建议同时运行 30 个以上的作业。

在 **Active IQ Unified Manager** 中查看卷保护状态

Data Protection 页面显示了单个群集中所有受保护卷或数据中心中所有群集的数据保护详细信息的整体视图。

步骤

1. 在左侧导航窗格中，单击*仪表板*。
2. 根据您是要查看所有受监控集群还是单个集群的数据保护状态，选择 所有集群 或从下拉菜单中选择单个集群。
3. 单击数据保护面板顶端的右箭头。此时将显示*数据保护*页面。

根据您是在数据中心中选择单个集群还是所有集群，此页面显示受 Snapshot 副本或 SnapMirror 策略保护的卷的数据保护状态，并显示未受保护的卷的计数。

从*单个集群*列表中选择集群将显示该集群中受保护卷的快照保护和 SnapMirror 关系状态。

单击此页面上的事件将转到事件详细信息页面。您可以单击 查看全部 链接，在事件管理清单页面中查看所有活动的保护事件。您可以悬停鼠标以查看相应的计数和图例。您可以单击：

- 未受保护卷和受 Snapshot 副本保护的卷的条形图，转到“卷”页面并查看详细信息。
- 所有关系的条形图可转到“关系”页面，其中的详细信息按源集群进行筛选。

查看受 **Snapshot** 副本保护的卷的保护状态

Snapshot 副本概述：受 Snapshot 副本保护的卷的概述，例如：

- 受 Snapshot 副本保护和不受 Snapshot 副本保护的卷总数。
- 正在使用或超过 Snapshot 副本保留空间的卷总数。

*快照副本分析*详细说明了以下信息：

- Snapshot 副本的单个事件，包括过去 24 小时内引发的事件。
- 受 Snapshot 副本保护和不受 Snapshot 副本保护的卷的详细图表。
- 使用、未使用以及超出保留的 Snapshot 副本容量的卷。
- 按 Snapshot 副本数量划分的卷计数细分。

Snapshot 副本注意事项

- 在计算受 Snapshot 副本保护的卷时，会同时考虑源卷和目标卷。
- 返回的 Snapshot 副本数仅适用于在线且可用的卷。
- Snapshot 副本数量的图形范围是动态的。它是基于选定集群中存在的快照数量生成的。
- 要将卷视为受保护的卷，应启用卷的 Snapshot 副本的计划。
- Snapshot 副本保留空间的值对于查看已使用的磁盘空间量或计算删除一个或多个 Snapshot 副本时可回收的空间非常重要。

查看 **SnapMirror** 关系的保护状态

SnapMirror 概述：受 SnapMirror 策略保护的卷的概述，例如：

- 受相应 SnapMirror 策略保护的卷数，例如卷 SnapMirror 关系、存储虚拟机灾难恢复（SVM-DR）及其组合。

- 基于滞后状态出现恢复点目标（RPO）滞后的 SnapMirror 关系总数。

*SnapMirror 分析*详细说明了以下信息：

- 为 SnapMirror 关系引发的各个事件，包括过去 24 小时内引发的事件
- 由每种类型的 SnapMirror 策略保护的卷数。
- 受 SnapMirror 关系类型（如 Asynchronous Mirror、Asynchronous Vault、Asynchronous MirrorVault 、StricxtSync、SnapMirror active sync consistency group 和 Sync）保护的关系数。
- 健康和不健康关系的数量。
- 卷关系计数的细分。您可以按 RPO 延迟时间和状态切换图表。
- 非托管关系的延迟阈值。您可以单击设置图标（ ）来配置延迟阈值设置。有关详细信息，请参见"配置非托管保护关系的滞后阈值设置"。

SnapMirror 关系的注意事项

- 在计算 SnapMirror 关系时，将计算已启用读写的源卷。不考虑目标卷和根卷。
- 对于 SnapMirror 关系，将显示源集群的事件。
- SnapMirror 关系计数包括源和目标位于相同或不同集群上的卷数量。
- 数据复制中 RPO 延迟的延迟持续时间基于 SnapMirror 关系。根据设置的关系阈值，状态分为 `ok`、`warning`或 `error`。您可以查看状态以确定参数是否按预期工作，或者是否需要解决任何问题。
- 如果卷有多个 SnapMirror 关系，则每个关系类型都计入 RPO 延迟。
- 如果源和目标之间的数据复制存在问题，例如，当关系断开时，则认为卷关系不正常。

查看受 **MetroCluster** 配置保护的集群

*数据保护*页面上的 *MetroCluster 保护*面板显示了您的站点上受基于 FC 或 IP 配置的 MetroCluster 保护或未受其保护的集群数量。单击此面板上的条形图将转到“集群”页面，其中根据受保护或未受保护的集群筛选集群详细信息。有关监控 MetroCluster 配置的信息，请参见 "监控 MetroCluster 配置"。

在 **Active IQ Unified Manager** 中查看卷保护关系

从“关系：所有关系”视图和“卷关系”页面，您可以查看现有卷 SnapMirror 和 SnapVault 关系的状态。您还可以查看有关保护关系的详细信息，包括传输和延迟状态、源和目标详细信息、计划和策略信息等。

开始之前

您必须具有应用程序管理员或存储管理员角色。

您也可以从此页面启动关系命令。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 从视图菜单中，选择 关系 > 所有关系。

此时将显示“关系：所有关系”视图。

3. 从下列方法中选择一种，以查看卷保护详细信息：
   - 要查看有关所有卷关系的当前信息，请停留在默认的*所有关系*页面上。
   - 要查看有关一段时间内卷传输趋势的详细信息，请在“视图”菜单中选择“关系：过去 1 个月传输状态”视图。
   - 要查看每天的卷传输活动的详细信息，请在“查看”菜单中选择“关系：过去 1 个月的传输速率”视图。

   卷传输视图仅显示异步关系中的卷的信息，不显示同步关系中的卷。

在 **Active IQ Unified Manager** 中监控一致性组 **LUN** 关系

如果您的 ONTAP 环境支持 SnapMirror 主动同步以保护具有 LUN 的应用程序，则可以在 Active IQ Unified Manager 上查看和监控这些 LUN。

SnapMirror 主动同步可确保在 SAN 环境中故障转移期间实现零恢复时间目标（RTO）。在支持 SnapMirror 主动同步的典型部署中，卷上的 LUN 受一致性组关系保护。

这些主 LUN 和辅助 LUN 是复合 LUN，或者是具有相同 UUID 和序列号的副本 LUN 对。I/O 操作（读取和写入）在这些复合 LUN 上的源站点和目标站点之间进行多路复用，以确保透明度。

要查看复合 LUN，应在 Unified Manager 上添加并发现包含属于一致性组关系的 LUN 的主集群和辅助集群。仅支持 iSCSI 和 FCP LUN。

有关 SnapMirror 活动同步的信息，请参见 "ONTAP 9 SnapMirror 活动同步文档（以前称为 SM-BC）"。

要查看环境中的复合 LUN，请按照以下步骤操作：

步骤

1. 在左侧导航窗格中，单击*存储* > **LUN**。
2. 在视图菜单中，选择 关系 > 所有 **LUN**。

   此时将显示 Relationship: All LUNs 视图。

您可以查看 LUN 详细信息，例如 LUN 名称、卷、托管 LUN 的存储 VM、集群、一致性组和配对 LUN。您可以单击这些组件中的每一个以深入查看详细视图。单击一致性组将转到“关系”页面。

通过单击伙伴 LUN，您可以在托管伙伴 LUN 的存储 VM 的 Storage VM Details 页面的 SAN 选项卡上查看其配置详细信息。此时将显示启动器和启动器组以及伙伴 LUN 的其他方面等信息。

您可以执行标准网格级功能，对环境中的受保护 LUN 进行排序、筛选、生成和上传报告。

在 **Active IQ Unified Manager** 的 **Health: All Volumes** 视图中创建 **SnapVault** 关系

您可以使用“运行状况：所有卷”视图为同一 Storage VM 上的一个或多个卷创建 SnapVault 关系，以启用用于保护目的的数据备份。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

在以下情况下，*保护*菜单不会显示：

- 如果 RBAC 设置不允许此操作：例如，如果您只有操作员权限
- 当卷 ID 未知时：例如，当您具有集群间关系并且尚未发现目标集群时

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在*运行状况：所有卷*视图中，选择要保护的卷，然后单击*保护*。

   或者，要在同一存储虚拟机 (SVM) 上创建多个保护关系，请在运行状况：所有卷视图中选择一个或多个卷，然后单击工具栏上的 保护。

3. 从菜单中选择 **SnapVault**。

   此时将启动“配置保护”对话框。

4. 单击 **SnapVault** 以查看 **SnapVault** 选项卡并配置辅助卷信息。
5. 单击*高级*根据需要设置重复数据删除、压缩、自动增长和空间保证，然后单击*应用*。
6. 在 **SnapVault** 选项卡中完成 目的地信息 区域和 关系设置 区域。
7. 单击*应用*。

   您将返回到“运行状况：所有卷”视图。

8. 单击 运行状况：所有卷 视图顶部的保护配置作业链接。

   如果仅创建一个保护关系，则会显示作业详细信息页面；但是，如果创建多个保护关系，则会显示与保护操作关联的所有作业的筛选列表。

9. 执行以下操作之一：
   - 如果您只有一个作业，请单击*刷新*以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。
   - 如果您有多个作业：
     i. 单击作业列表中的作业。
     ii. 单击*刷新*以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。
     iii. 使用*返回*按钮返回筛选列表并查看另一个作业。

在 **Active IQ Unified Manager** 的 **Volume/Health** 详细信息页面中创建 **SnapVault** 保护关系

您可以使用“卷/运行状况详细信息”页面创建 SnapVault 关系，以便在卷上启用数据备份以进行保护。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation 才能执行此任务。

在以下情况下，*保护*菜单不会显示：

- 如果 RBAC 设置不允许此操作：例如，如果您只有操作员权限
- 当卷 ID 未知时：例如，当您具有集群间关系并且尚未发现目标集群时

步骤

1. 在*卷/运行状况*详细信息页面的*保护*选项卡中，右键单击拓扑视图中要保护的卷。
2. 从菜单中选择 保护 > **SnapVault**。

   此时将启动“配置保护”对话框。

3. 单击 **SnapVault** 可查看 **SnapVault** 选项卡并配置辅助资源信息。
4. 单击*高级*根据需要设置重复数据删除、压缩、自动增长和空间保证，然后单击*应用*。
5. 在*配置保护*对话框中填写*目标信息*区域和*关系设置*区域。
6. 单击*应用*。

   将返回到卷/运行状况详细信息页面。

7. 单击 **Volume / Health** 详细信息页面顶部的保护配置作业链接。

   此时将显示作业详细信息页面。

8. 单击*刷新*以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。

   作业任务完成后，新的关系将显示在卷/运行状况详细信息页面拓扑视图中。

在 **Active IQ Unified Manager** 的 **Health: All Volumes** 视图中创建 **SnapMirror** 关系

使用“运行状况：所有卷”视图，您可以通过在同一存储 VM 上选择多个卷来一次创建多个 SnapMirror 保护关系。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

在以下情况下，*保护*菜单不会显示：

- 如果 RBAC 设置不允许此操作：例如，如果您只有操作员权限
- 当卷 ID 未知时：例如，当您具有集群间关系并且尚未发现目标集群时

步骤

1. 在*运行状况：所有卷*视图中，选择要保护的卷。

   或者，要在同一 SVM 上创建多个保护关系，请在“运行状况：所有卷”视图中选择一个或多个卷，然后单击

工具栏上的 保护 > **SnapMirror**。

此时将显示配置保护对话框。

2. 单击 **SnapMirror** 以查看 **SnapMirror** 选项卡并配置目标信息。
3. 单击*高级*以根据需要设置空间保障，然后单击*应用*。
4. 完成 **SnapMirror** 选项卡中的 目的地信息 区域和 关系设置 区域。
5. 单击*应用*。

   您将返回到“运行状况：所有卷”视图。

6. 单击*运行状况：所有卷视图*顶部的保护配置作业链接。

   如果仅创建一个保护关系，则会显示作业详细信息页面；但是，如果创建多个保护关系，则会显示与保护操作关联的所有作业的列表。

7. 执行以下操作之一：
   - 如果您只有一个作业，请单击*刷新*以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。
   - 如果您有多个作业：
     i. 单击作业列表中的作业。
     ii. 单击*刷新*以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。
     iii. 使用*返回*按钮返回筛选列表并查看另一个作业。

根据在配置过程中指定的目标 SVM 或在高级设置中启用的选项，生成的 SnapMirror 关系可能是以下几种可能的变体之一：

- 如果您指定的目标 SVM 运行的 ONTAP 版本与源卷相同或比其更新，则默认结果为基于块复制的 SnapMirror 关系。
- 如果您指定的目标 SVM 运行的 ONTAP 版本与源卷相同或比源卷更新，但您在高级设置中启用了版本灵活的复制，则会产生具有版本灵活复制功能的 SnapMirror 关系。
- 如果您指定的目标 SVM 运行的 ONTAP 版本早于源卷，并且该早期版本支持版本灵活的复制，则会自动生成具有版本灵活复制功能的 SnapMirror 关系。

从 **Active IQ Unified Manager** 中的卷健康状况详细信息页面创建 **SnapMirror** 关系

您可以使用“卷/运行状况详细信息”页面创建 SnapMirror 关系，以便为保护目的启用数据复制。SnapMirror 复制使您能够在源数据丢失的情况下从目标卷还原数据。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

在以下情况下，*保护*菜单不会显示：

- 如果 RBAC 设置不允许此操作：例如，如果您只有操作员权限

- 当卷 ID 未知时：例如，当您具有集群间关系并且尚未发现目标集群时

您最多可以同时执行 10 个保护作业，而不会影响性能。当您同时运行 11 到 30 个作业时，可能会遇到一些性能影响。不建议同时运行 30 个以上的作业。

步骤

1. 在*卷/运行状况*详细信息页面的*保护选项卡*中，右键单击拓扑视图中要保护的卷的名称。
2. 从菜单中选择 保护 > **SnapMirror**。

   此时将显示配置保护对话框。
3. 单击 **SnapMirror** 以查看 **SnapMirror** 选项卡并配置目标信息。
4. 单击*高级*以根据需要设置空间保障，然后单击*应用*。
5. 在*配置保护*对话框中填写*目标信息*区域和*关系设置*区域。
6. 单击*应用*。

   将返回到卷/运行状况详细信息页面。
7. 单击 **Volume / Health** 详细信息页面顶部的保护配置作业链接。

   作业的任务和详细信息显示在作业详细信息页面中。
8. 在*作业*详细信息页面中，单击*刷新*以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。
9. 作业任务完成后，单击浏览器上的 返回 以返回 卷 / 运行状况 详细信息页面。

   新关系将显示在卷/运行状况详细信息页面拓扑视图中。

根据在配置过程中指定的目标 SVM 或在高级设置中启用的选项，生成的 SnapMirror 关系可能是以下几种可能的变体之一：

- 如果您指定的目标 SVM 运行的 ONTAP 版本与源卷相同或比其更新，则默认结果为基于块复制的 SnapMirror 关系。
- 如果您指定的目标 SVM 运行的 ONTAP 版本与源卷相同或比源卷更新，但您在高级设置中启用了版本灵活的复制，则会产生具有版本灵活复制功能的 SnapMirror 关系。
- 如果您指定的目标 SVM 运行的是早期版本的 ONTAP，或者版本高于源卷的版本，并且早期版本支持版本灵活复制，则会自动生成具有版本灵活复制功能的 SnapMirror 关系。

在 **Active IQ Unified Manager** 中创建具有版本灵活复制功能的 **SnapMirror** 关系

您可以使用版本灵活的复制创建 SnapMirror 关系。版本灵活的复制使您能够实施 SnapMirror 保护，即使源卷和目标卷运行不同版本的 ONTAP。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

- 源和目标 SVM 都必须启用 SnapMirror 许可证。
- 源和目标 SVM 必须各自在支持版本灵活复制的 ONTAP 软件版本下运行。

采用版本灵活复制的 SnapMirror 使您即使在并非所有存储都运行在同一版本 ONTAP 下的异构存储环境中，也能实施 SnapMirror 保护；但是，在采用版本灵活复制的 SnapMirror 下执行的镜像操作，其执行速度不如在传统数据块复制 SnapMirror 下执行得快。

步骤

1. 显示要保护的卷的*配置保护*对话框。
   - 如果正在查看“卷/运行状况详细信息”页面的“保护”选项卡，请在具有要保护的卷名称的拓扑视图中单击鼠标右键，然后从菜单中选择 保护 > **SnapMirror**。
   - 如果正在查看“运行状况：所有卷”视图，请找到要保护的卷并右键单击它；然后从菜单中选择 保护 > **SnapMirror**。此时将显示“配置保护”对话框。
2. 单击 **SnapMirror** 以查看 **SnapMirror** 选项卡。
3. 在*配置保护*对话框中填写*目标信息*区域和*关系设置*区域。

   如果指定的目标 SVM 运行的 ONTAP 版本早于您要保护的源卷，并且该早期版本支持版本灵活的复制，则此任务会自动将 SnapMirror 配置为使用版本灵活的复制。
4. 如果您指定的目标 SVM 运行的 ONTAP 版本与源卷相同，但您仍希望配置具有版本灵活复制功能的 SnapMirror，请单击 高级 以启用版本灵活的复制，然后单击 应用。
5. 单击*应用*。

   将返回到卷/运行状况详细信息页面。
6. 单击 **Volume / Health** 详细信息页面顶部的保护配置作业链接。

   作业任务和详细信息显示在作业详细信息页面中。
7. 在*作业*详细信息页面中，单击*刷新*以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。
8. 作业任务完成后，单击浏览器上的 返回 以返回 卷 / 运行状况 详细信息页面。

   新关系将显示在卷/运行状况详细信息页面拓扑视图中。

在 **Active IQ Unified Manager** 中创建具有版本灵活复制和回退选项功能的 **SnapMirror** 关系

您可以使用版本灵活的复制和备份选项功能创建 SnapMirror 关系。备份选项功能使您能够实施 SnapMirror 保护，并在目标位置保留多个版本的备份副本。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。
- 源和目标 SVM 都必须启用 SnapMirror 许可证。
- 源和目标 SVM 都必须启用 SnapVault 许可证。

- 源和目标 SVM 必须各自在支持版本灵活复制的 ONTAP 软件版本下运行。

通过配置 SnapMirror 备份选项功能，您可以使用 SnapMirror 灾难恢复功能（如卷故障切换功能）来保护数据，同时提供多个备份副本保护等 SnapVault 功能。

步骤

1. 显示要保护的卷的*配置保护*对话框。
   - 如果正在查看“卷/运行状况详细信息”页面的“保护”选项卡，请在拓扑视图中右键单击要保护的卷的名称，然后从菜单中选择 保护 > **SnapMirror**。
   - 如果您正在查看“运行状况：所有卷”视图，请找到要保护的卷并右键单击它；然后从菜单中选择 保护 > **SnapMirror**。此时将显示“配置保护”对话框。
2. 单击 **SnapMirror** 以查看 **SnapMirror** 选项卡。
3. 在*配置保护*对话框中填写*目标信息*区域和*关系设置*区域。
4. 单击*高级*以显示*高级目标设置*对话框。
5. 如果尚未选中*版本灵活复制*复选框，请立即选中它。
6. 选中 **With backup option** 复选框以启用备份选项功能；然后单击 **Apply**。
7. 单击*应用*。

   将返回到卷/运行状况详细信息页面。
8. 单击 **Volume / Health** 详细信息页面顶部的保护配置作业链接。

   作业任务和详细信息显示在作业详细信息页面中。
9. 在*作业*详细信息页面中，单击*刷新*以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。
10. 作业任务完成后，单击浏览器上的 返回 以返回 卷 / 运行状况 详细信息页面。

    新关系将显示在卷/运行状况详细信息页面拓扑视图中。

在 **Active IQ Unified Manager** 中配置目标效率设置

您可以使用“高级目标设置”对话框在保护目标上配置目标效率设置，例如重复数据删除、压缩、自动增长和空间保证。如果要最大限度地提高目标卷或辅助卷上的空间利用率，请使用这些设置。

开始之前

您必须具有应用程序管理员或存储管理员角色。

默认情况下，效率设置与源卷的效率设置相匹配，但 SnapVault 关系中的压缩设置除外，这些设置默认情况下处于禁用状态。

步骤

1. 在 **Configure Protection** 对话框中单击 **SnapMirror** 选项卡或 **SnapVault** 选项卡，具体取决于您要配置的关系类型。

2. 单击*目标信息*区域中的*高级*。

   此时将打开高级目标设置对话框。

3. 根据需要启用或禁用重复数据删除、数据压缩、自动增长和空间保证的效率设置。
4. 单击*应用*以保存选择并返回到*配置保护*对话框。

在 **Active IQ Unified Manager** 中创建 **SnapMirror** 和 **SnapVault** 计划

您可以创建基本或高级 SnapMirror 和 SnapVault 计划，以启用源卷或主卷上的自动数据保护传输，以便更频繁或更少地进行传输，具体取决于卷上的数据更改频率。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已完成“配置保护”对话框中的“目标信息”区域。
- 您必须已设置 Workflow Automation 才能执行此任务。

步骤

1. 在*配置保护*对话框的 **SnapMirror** 选项卡或 **SnapVault** 选项卡中，单击*关系设置*区域中的*创建计划*链接。

   此时将显示创建计划对话框。

2. 在*计划名称*字段中，键入要为计划提供的名称。
3. 选择以下选项之一：
   - 基本

     选择是否要创建基本间隔样式计划。

   - 高级

     选择是否要创建 cron 样式计划。

4. 单击 **Create**。

   新计划显示在 SnapMirror 计划或 SnapVault 计划下拉列表中。

使用 **Active IQ Unified Manager** 中的级联或扇出关系扩展保护

您可以通过从源卷创建扇出或从现有关系的目标卷创建级联来扩展现有关系的保护。当您需要将数据从一个站点复制到多个站点或通过创建更多备份来提供额外保护时，可以执行此操作。

您可以使用一致性组将保护扩展到卷，一致性组是容纳多个卷的容器，因此您可以将所有卷作为一个实体进行管理。您可以在 Unified Manager 的“关系”页面中查看 SnapMirror 活动同步一致性组和同步一致性组关系。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

步骤

1. 单击*保护* > 关系。或者，您可以从卷详细信息页面查看关系。
2. 从*卷关系*页面中，选择要从中扩展保护的 SnapMirror 关系。
3. 在操作栏上，单击*扩展保护*。
4. 在菜单中，选择*从源*或*从目标*，具体取决于您是从源创建扇出关系还是从目标创建级联关系。
5. 根据您要创建的保护关系类型，选择 **With SnapMirror** 或 **With SnapVault**。

   此时将显示*配置保护*对话框。

   这可以从统一关系 / 卷关系和卷 / 运行状况详细信息页面实现。

6. 按照*配置保护*对话框中的指示填写信息。

从 **Active IQ Unified Manager** 的卷关系页面编辑保护关系

您可以编辑现有的保护关系，以更改最大传输速率、保护策略或保护计划。您可能会编辑关系以减少用于传输的带宽，或者因为数据经常发生变化而增加计划传输的频率。

开始之前

您必须具有应用程序管理员或存储管理员角色。

所选卷必须是保护关系目标。如果选择了源卷、负载分担卷或非 SnapMirror 或 SnapVault 关系目标的卷，则无法编辑关系。

步骤

1. 从*卷关系*页面中，在卷列表中选择要编辑关系设置的相同 SVM 中的一个或多个卷，然后从工具栏中选择*编辑*。

   此时将显示编辑关系对话框。

2. 在*编辑关系*对话框中，根据需要编辑最大传输速率、保护策略或保护计划。
3. 单击*应用*。

   更改将应用于所选关系。

从 **Active IQ Unified Manager** 中的卷/运行状况详细信息页面编辑保护关系

您可以编辑现有的保护关系，以更改当前的最大传输速率、保护策略或保护计划。您可能需要编辑关系以减少用于传输的带宽，或者因为数据经常更改而增加计划传输的频率。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

- 您必须已安装并配置 Workflow Automation。

所选卷必须是保护关系目标。如果选择了源卷、负载分担卷或非 SnapMirror 或 SnapVault 关系目标的卷，则无法编辑关系。

步骤

1. 从*卷/运行状况*详细信息页面的*保护*选项卡中，在拓扑中找到要编辑的保护关系，然后右键单击它。
2. 从菜单中选择*编辑*。

   或者，从*操作*菜单中，选择*关系* > *编辑*以编辑您当前查看详细信息的关系。

   此时将显示*编辑关系*对话框。
3. 在编辑关系对话框中，根据需要编辑最大传输速率、保护策略或保护计划。
4. 单击*应用*。

   更改将应用于所选关系。

创建 **SnapMirror** 策略以在 **Active IQ Unified Manager** 中最大化传输效率

您可以创建 SnapMirror 策略来指定保护关系的 SnapMirror 传输优先级。SnapMirror 策略使您能够通过分配优先级来最大限度地提高从源到目标的传输效率，以便计划在正常优先级传输之后运行较低优先级的传输。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。
- 此任务假定您已完成“配置保护”对话框中的“目标信息”区域。

步骤

1. 在*配置保护*对话框的 **SnapMirror** 选项卡中，单击*关系设置*区域中的*创建策略*链接。

   此时将显示创建 SnapMirror 策略对话框。
2. 在*策略名称*字段中，键入要为策略指定的名称。
3. 在*传输优先级*字段中，选择要分配给策略的传输优先级。
4. 在 **Comment** 字段中，为策略输入可选注释。
5. 单击 **Create**。

   新策略将显示在“SnapMirror 策略”下拉列表中。

在 **Active IQ Unified Manager** 中创建 **SnapVault** 策略以最大限度地提高传输效率

您可以创建新的 SnapVault 策略来设置 SnapVault 传输的优先级。您可以使用策略来最大限度地提高保护关系中从主端到二级端的传输效率。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。
- 您必须已完成“配置保护”对话框中的“目标信息”区域。

步骤

1. 在*配置保护*对话框的*SnapVault*选项卡中，单击*关系设置*区域中的*创建策略*链接。

   此时将显示 SnapVault 选项卡。

2. 在*策略名称*字段中，键入要为策略指定的名称。
3. 在*传输优先级*字段中，选择要分配给策略的传输优先级。
4. 可选： 在 注释 字段中，输入策略的注释。
5. 在*复制标签*区域中，根据需要添加或编辑复制标签。
6. 单击 **Create**。

   新策略显示在“创建策略”下拉列表中。

从 **Active IQ Unified Manager** 的卷关系页面中止传输

如果要停止正在进行的 SnapMirror 复制，可以中止活动数据保护传输。您还可以清除基线传输之后的传输的重新启动检查点。当传输与其他操作（如卷移动）冲突时，您可以中止传输。

无法中止受一致性组保护的卷关系。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

在以下情况下，中止操作不会显示：

- 如果 RBAC 设置不允许此操作：例如，如果您只有操作员权限
- 当卷 ID 未知时：例如，当您具有集群间关系并且尚未发现目标集群时

无法清除基线传输的重新启动检查点。

步骤

1. 要中止一个或多个保护关系的传输，请从*卷关系*页面中选择一个或多个卷，然后在工具栏上单击*中止*。

   此时将显示中止传输对话框。

2. 如果要清除非基线传输的重启检查点，请选择*清除检查点*。
3. 单击*继续*。

“中止传输”对话框已关闭，中止作业的状态将显示在“卷关系”页面的顶部，以及指向作业详细信息的链接。

4. *可选：*单击*查看详细信息*链接转到*作业*详细信息页面，以获取更多详细信息并查看作业进度。

从 **Active IQ Unified Manager** 的卷/运行状况详细信息页面中止传输

如果要停止正在进行的 SnapMirror 复制，您可以中止活动的数据保护传输。如果不是基线传输，您还可以清除传输的重新启动检查点。当传输与其他操作（例如卷移动）冲突时，您可能需要中止传输。

无法中止受一致性组保护的卷关系。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

在以下情况下，中止操作不会显示：

- 如果 RBAC 设置不允许此操作：例如，如果您只有操作员权限
- 当卷 ID 未知时：例如，当您具有集群间关系并且尚未发现目标集群时

无法清除基线传输的重新启动检查点。

步骤

1. 在*卷/健康*详细信息页面的*保护*选项卡中，在拓扑视图中右键单击要中止数据传输的关系，然后选择*中止*。

   此时将显示中止传输对话框。

2. 如果要清除非基线传输的重启检查点，请选择*清除检查点*。
3. 单击*继续*。

   “中止传输”对话框已关闭，中止操作的状态将显示在“卷/运行状况详细信息”页面的顶部，并显示指向作业详细信息的链接。

4. *可选：*单击*查看详细信息*链接转到*作业*详细信息页面，以获取更多详细信息并查看作业进度。
5. 单击每个作业任务以查看其详细信息。
6. 单击浏览器上的后退箭头，返回 **Volume / Health** 详细信息页面。

   当所有作业任务成功完成时，中止操作完成。

从 **Active IQ Unified Manager** 的卷关系页面暂停保护关系

从“卷关系”页面，您可以暂停保护关系，以暂时阻止发生数据传输。当您要为包含数据库的 SnapMirror 目标卷创建 Snapshot 副本，并且希望确保在 Snapshot 副本操作期间其内容稳定时，您可以暂停关系。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

在以下情况下不会显示静止操作：

- 如果 RBAC 设置不允许此操作；例如，如果您只有操作员权限
- 当卷 ID 未知时；例如，当您具有集群间关系并且尚未发现目标集群时
- 未配对 Workflow Automation 和 Unified Manager 时

步骤

1. 要静默一个或多个保护关系的传输，请从*卷关系*页面中选择一个或多个卷，然后在工具栏上单击*静默*。

   此时将显示静默对话框。

2. 单击*继续*。

   静止作业的状态将显示在“卷/运行状况详细信息”页面的顶部，并提供指向作业详细信息的链接。

3. 单击*查看详细信息*链接转到*作业*详细信息页面以获取更多详细信息和作业进度。
4. *可选：*单击浏览器上的*后退*箭头返回*卷关系*页面。

   当所有作业任务成功完成时，静默作业即告完成。

从 **Active IQ Unified Manager** 中的卷/运行状况详细信息页面静默保护关系

您可以暂停保护关系，以暂时阻止发生数据传输。当您要为包含数据库的 SnapMirror 目标卷创建 Snapshot 副本，并且希望确保其内容在 Snapshot 副本期间保持稳定时，您可以暂停关系。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

在以下情况下不会显示静止操作：

- RBAC 设置不允许执行此操作，例如您只有操作员权限
- 卷 ID 未知，例如，您有一个集群间关系，但尚未发现目标集群
- 未配对 Workflow Automation 和 Unified Manager 时

步骤

1. 在 卷/运行状况 详细信息页面的 保护 选项卡中，在拓扑视图中右键单击要暂停的保护关系。
2. 从菜单中选择*静止*。
3. 单击 **Yes** 继续。

   静止作业的状态将显示在“卷/运行状况详细信息”页面的顶部，并提供指向作业详细信息的链接。

4. 单击*查看详细信息*链接转到*作业*详细信息页面以获取更多详细信息和作业进度。
5. 可选： 单击浏览器上的后退箭头返回 卷/运行状况 详细信息页面。

   当所有作业任务成功完成时，静默作业即告完成。

从 **Active IQ Unified Manager Volume Relationships** 页面中断 **SnapMirror** 关系

您可以中断保护关系，以停止 SnapMirror 关系中的源卷和目标卷之间的数据传输。当您想要迁移数据、进行灾难恢复或进行应用程序测试时，您可能会中断关系。目标卷将更改为读/写卷。您无法中断 SnapVault 关系。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

步骤

1. 从*卷关系*页面中，选择一个或多个具有要停止数据传输的保护关系的卷，然后在工具栏上单击*中断*。

   此时将显示断开关系对话框。

2. 单击*继续*以中断此关系。
3. 在 **Volume Relationships** 页面的 **Relationship State** 列中，确认关系已断开。

   默认情况下，关系状态列是隐藏的，因此您可能需要在显示/隐藏列列表中选择它 。

从 **Active IQ Unified Manager** 的卷关系页面删除保护关系

在“卷关系”页面中，您可以删除保护关系，以永久删除所选源和目标之间的现有关系：例如，当您希望使用其他目标创建关系时。此操作将删除所有元数据，并且无法撤消。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

步骤

1. 从*卷关系*页面中，选择一个或多个具有要删除的保护关系的卷，然后在工具栏上单击*删除*。

   此时将显示删除关系对话框。

2. 单击*继续*删除此关系。

   该关系将从“卷关系”页面中删除。

从 **Active IQ Unified Manager** 的卷关系页面恢复已暂停关系上的计划传输

停顿关系以停止计划传输后，您可以使用 恢复 重新启用计划传输，以保护源卷或主卷上的数据。如果存在检查点，则在下一个计划传输间隔从检查点恢复传输。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

您最多只能选择 10 个已静默的关系来恢复传输。

步骤

1. 从 Volume **Relationships** 页面中，选择一个或多个具有已静默关系的卷，然后在工具栏上单击 **Resume**。
2. 在 **Resume** 对话框中，单击 **Continue**。

   您将返回到“卷关系”页面。

3. 要查看相关作业任务并跟踪其进度，请单击*卷关系*页面顶部显示的作业链接。
4. 执行以下操作之一：
   - 如果仅显示一个作业，请在作业详细信息页面中单击*刷新*以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。
   - 如果显示多个作业，
     i. 在作业页面中，单击要查看其详细信息的作业。
     ii. 在作业详细信息页面中，单击 刷新 以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。作业完成后，数据传输将在下一个计划传输间隔恢复。

从 **Active IQ Unified Manager** 的"卷/运行状况详细信息"页面恢复已静默关系上的传输

在停顿关系以停止发生计划传输后，您可以使用卷/运行状况详细信息页面上的*恢复*重新启用计划传输，以便保护源卷或主卷上的数据。在下一个计划传输间隔，传输将从检查点（如果存在）恢复。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。

步骤

1. 在*卷/运行状况*详细信息页面的*保护*选项卡中，右键单击拓扑视图中要恢复的已停顿关系。

   或者，从*操作* > 关系*菜单中选择*恢复。

2. 在 **Resume** 对话框中，单击 **Continue**。

   将返回到卷/运行状况详细信息页面。

3. 要查看相关作业任务并跟踪其进度，请单击显示在 **Volume / Health** 详细信息页面顶部的作业链接。
4. 在*作业*详细信息页面中，单击*刷新*以更新与保护配置作业关联的任务列表和任务详细信息，并确定作业何时完成。

   作业完成后，数据传输将在下一计划传输间隔恢复。

从 **Active IQ Unified Manager** 中的卷关系页面初始化或更新保护关系

在“卷关系”页面中，您可以对新的保护关系执行首次基线传输，或者在关系已初始化且您希望执行手动、计划外的增量更新以立即进行传输时，更新该关系。

无法初始化或更新受一致性组保护的卷。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 OnCommand Workflow Automation。

步骤

1. 在*卷关系*页面中，右键单击卷，并选择一个或多个具有要更新或初始化的关系的卷，然后在工具栏上单击*初始化/更新*。

   此时将显示*初始化/更新*对话框。

2. 在*传输选项*选项卡中，选择传输优先级和最大传输速率。
3. 单击*源 Snapshot 副本*；然后，在*Snapshot 副本*列中，单击*默认*。

   此时将显示选择源 Snapshot 副本对话框。

4. 如果要指定现有 Snapshot 副本而不是传输默认 Snapshot 副本，请单击 现有 **Snapshot** 副本 并从列表中选择 Snapshot 副本。
5. 单击*提交*。

   您将返回到*初始化/更新*对话框。

6. 如果选择了多个要初始化或更新的源，请单击要指定现有 Snapshot 副本的下一个源的 默认。
7. 单击*提交*以开始初始化或更新作业。

   初始化或更新作业已启动，您将返回到卷关系页面，并在页面顶部显示作业链接。

8. 可选： 单击 健康：所有卷 视图上的 查看作业 以跟踪每个初始化或更新作业的状态。

   此时将显示已筛选的作业列表。

9. 可选： 单击每个作业以查看其详细信息。
10. *可选：*单击浏览器上的*后退*箭头返回*卷关系*页面。

    当所有任务成功完成时，初始化或更新操作完成。

从 **Active IQ Unified Manager** 中的卷/运行状况详细信息页面初始化或更新保护关系

您可以对新的保护关系执行首次基线传输，或者在关系已初始化且您希望执行手动的计划外增量更新以立即传输数据时更新该关系。

注意：无法初始化或更新受一致性组保护的卷。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 OnCommand Workflow Automation。

步骤

1. 从*卷/运行状况*详细信息页面的*保护*选项卡中，在拓扑中找到要初始化或更新的保护关系，然后右键单击它。
2. 从菜单中选择*初始化/更新*。

   或者，从*操作*菜单中，选择*关系* > *初始化/更新*以初始化或更新您当前正在查看其详细信息的关系。

   此时将显示初始化/更新对话框。
3. 在*传输选项*选项卡中，选择传输优先级和最大传输速率。
4. 单击*源 Snapshot 副本*；然后，在*Snapshot 副本*列中，单击*默认*。

   此时将显示选择源 Snapshot 副本对话框。
5. 如果要指定现有 Snapshot 副本而不是传输默认 Snapshot 副本，请单击 现有 **Snapshot** 副本 并从列表中选择 Snapshot 副本。
6. 单击*提交*。

   此时将返回到“初始化/更新”对话框。
7. 如果选择了多个要初始化或更新的源，请针对要指定现有 Snapshot 副本的下一个读/写源单击 默认。

   您不能为数据保护卷选择其他 Snapshot 副本。
8. 单击*提交*以开始初始化或更新作业。

   初始化或更新作业已启动，您将返回到卷/运行状况详细信息页面，并在页面顶部显示作业链接。
9. 可选： 单击 卷/运行状况 详细信息页面上的 查看作业 以跟踪每个初始化或更新作业的状态。

   此时将显示已筛选的作业列表。
10. 可选： 单击每个作业以查看其详细信息。
11. 可选： 单击浏览器上的后退箭头返回 卷/运行状况 详细信息页面。

    当所有作业任务成功完成时，初始化或更新操作完成。

从 **Active IQ Unified Manager** 的卷关系页面重新同步保护关系

从“卷关系”页面中，您可以重新同步关系，以便从禁用源卷的事件中恢复，或者在要将当前源更改为其他卷时进行重新同步。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

- 您必须已设置 Workflow Automation。

步骤

1. 从 卷关系 页面中，选择一个或多个具有已静默关系的卷，然后从工具栏中单击 重新同步。

   此时将显示重新同步对话框。

2. 在*重新同步选项*选项卡中，选择传输优先级和最大传输速率。
3. 单击*源 Snapshot 副本*；然后，在*Snapshot 副本*列中，单击*默认*。

   此时将显示选择源 Snapshot 副本对话框。

4. 如果要指定现有 Snapshot 副本而不是传输默认 Snapshot 副本，请单击 现有 **Snapshot** 副本 并从列表中选择 Snapshot 副本。
5. 单击*提交*。

   此时将返回到“重新同步”对话框。

6. 如果选择了多个要重新同步的源，请单击要指定现有 Snapshot 副本的下一个源的 默认值。
7. 单击*提交*以开始重新同步作业。

   重新同步作业已启动，您将返回到卷关系页面，并在页面顶部显示作业链接。

8. 可选：*单击 *卷关系 页面上的 查看作业 以跟踪每个重新同步作业的状态。

   此时将显示已筛选的作业列表。

9. *可选：*单击浏览器上的*后退*箭头返回*卷关系*页面。

   当所有作业任务成功完成时，重新同步操作完成。

从 **Active IQ Unified Manager** 的"卷关系"页面反转保护关系

当灾难导致保护关系中的源卷不可用时，您可以在修复或更换源卷期间，通过将目标卷转换为读/写卷来使用它提供数据。当源再次可用于接收数据时，您可以使用反向重新同步操作反向建立关系，将源上的数据与读/写目标上的数据进行同步。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已设置 Workflow Automation。
- 此关系不得为 SnapVault 关系。
- 保护关系必须已存在。
- 必须中断保护关系。
- 源和目标必须处于联机状态。
- 源不能是其他数据保护卷的目标。
- 执行此任务时，源上比通用 Snapshot 副本上的数据更新的数据将被删除。

- 在反向重新同步关系上创建的策略和计划与原始保护关系上的策略和计划相同。

  如果策略和计划不存在，则会创建这些策略和计划。

步骤

1. 从*卷关系*页面中，选择一个或多个具有要反向的关系的卷，然后在工具栏上单击*反向重新同步*。

   此时将显示反向重新同步对话框。

2. 验证*反向重新同步*对话框中显示的关系是否是要执行反向重新同步操作的关系，然后单击*提交*。

   反向重新同步操作已启动，您将返回到卷关系页面，并在页面顶部显示作业链接。

3. 可选： 单击 卷关系 页面上的 查看作业 以跟踪每个反向重新同步作业的状态。

   此时将显示与此操作相关的作业筛选列表。

4. *可选：*单击浏览器上的*后退*箭头返回*卷关系*页面。

   当所有作业任务成功完成时，反向重新同步操作完成。

使用 **Active IQ Unified Manager** 中的卷和卷/运行状况详细信息页面还原数据

您可以使用卷和卷/运行状况详细信息页面上的还原功能从 Snapshot 副本还原覆盖或删除的文件、目录或整个卷。

开始之前

您必须具有应用程序管理员或存储管理员角色。

请注意以下几点：

- 在以下任何情况下，您都不能从快照还原目录或卷：
  - 已选择 **Yes, preserve all snapshot copies** 选项。
  - 您正在使用 LDAP 帐户来监控集群。
  - 您已以域用户身份登录。
  - 您的帐户已配置为进行 SAML 身份验证。
  - 您正在使用 NDMP 协议。

    有关详细信息，请参见 Knowledge Base 文章 "如何在 "SVM-scope" 模式下配置 NDMP 身份验证"。
- 您无法还原 NTFS 文件流。
- 在以下情况下，还原选项不可用：
  - 卷 ID 未知：例如，您有一个集群间关系，但尚未发现目标集群。
  - 已为此卷配置 SnapMirror 同步复制。

步骤

1. 在左侧导航窗格中，转到 存储 > 卷。
2. 选择卷，然后单击*还原*按钮。或者，单击该卷以转到*Volume / Health details > Actions > Restore*。此时将显示还原对话框。有关此页面的信息，请参阅 "还原对话框"。
3. 选择要从中还原数据的卷和 Snapshot 副本（如果它们与默认值不同）。
4. 选择要还原的项目，例如源 LUN。

   您可以还原整个卷，也可以指定要还原的文件夹和文件。

5. 选择要将所选项目还原到的位置：原始位置*或*备用现有位置。
6. 如果选择其他现有位置，请执行以下操作之一：
   - 在“还原路径”文本字段中，键入要还原数据的位置的路径，然后单击*选择目录*。
   - 单击*浏览*以启动“浏览目录”对话框并完成以下步骤：
     i. 选择要还原的目标群集、存储 VM（SVM）和卷。
     ii. 在名称表中，选择必须还原的目录名称。
     iii. 点击*选择目录*。
7. 单击 还原。

   还原过程开始。后端将创建一个作业以完成还原过程。

8. 如果要查看作业进度，请从左侧导航窗格导航到*保护 > 作业*，以从作业列表中查看还原作业的状态。

> 如果在 Cloud Volumes ONTAP HA 群集之间还原操作失败并出现 NDMP 错误，则可能需要在目标群集中添加显式 AWS 路由，以便目标可以与源系统的群集管理 LIF 进行通信。您可以使用 NetApp Console 执行此配置步骤。

了解 **Active IQ Unified Manager** 中的资源池

资源池是由存储管理员使用 Unified Manager 为合作伙伴应用程序提供调配以进行备份管理而创建的聚合组。

您可以根据性能、成本、物理位置或可用性等属性将资源池化。通过将相关资源分组到一个池中，您可以将该池视为一个单一单元来进行监控和配置。这简化了这些资源的管理，并使存储的使用更加灵活高效。

在辅助存储配置期间，Unified Manager 使用以下标准确定资源池中最适合保护的聚合：

- 此聚合为数据聚合（而非根聚合），并且处于联机状态。
- 聚合位于 ONTAP 版本等于或高于源集群主要版本的目标集群节点上。
- 此聚合在资源池中的所有聚合中具有最大的可用空间。
- 在配置目标卷后，聚合空间处于为聚合定义的几乎已满和几乎超额配置的阈值内（全局或本地阈值，以适用者为准）。
- 目标节点上的 FlexVol 卷数不得超过平台限制。

在 **Active IQ Unified Manager** 中创建资源池

您可以使用“创建资源池”对话框对聚合进行分组以进行配置。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

资源池可以包含来自不同群集的聚合，但相同的聚合不能属于不同的资源池。

1. 在左侧导航窗格中，单击 保护 > 资源池。
2. 在*资源池页面*中，单击*创建*。
3. 按照*创建资源池*对话框中的说明提供名称和描述，并将聚合作为成员添加到要创建的资源池。

在 **Active IQ Unified Manager** 中编辑资源池

当要更改资源池名称和描述时，可以编辑现有资源池。

开始之前

您必须具有应用程序管理员或存储管理员角色。

仅当选择了一个资源池时，才会启用*编辑*按钮。如果选择了多个资源池，则会禁用*编辑*按钮。

步骤

1. 在左侧导航窗格中，单击 保护 > 资源池。
2. 从列表中选择一个资源池。
3. 单击 **Edit**。

   此时将显示 Edit Resource Pool（编辑资源池）窗口。
4. 根据需要编辑资源池名称和描述。
5. 单击 **Save**。

   新名称和描述显示在资源池列表中。

在 **Active IQ Unified Manager** 中查看资源池清单

您可以使用“资源池”页面查看资源池清单并监视每个资源池的剩余容量。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击 保护 > 资源池。

   此时将显示资源池清单。

在 **Active IQ Unified Manager** 中添加资源池成员

资源池由多个成员聚合组成。您可以向现有资源池添加聚合，以增加可用于辅助卷配置的空间量。

开始之前

您必须具有应用程序管理员或存储管理员角色。

一次最多可向资源池添加 200 个聚合。“聚合”对话框中显示的聚合不属于任何其他资源池。

步骤

1. 在左侧导航窗格中，单击 保护 > 资源池。
2. 从*资源池*列表中选择一个资源池。

   资源池成员显示在资源池列表下方的区域中。
3. 在资源池成员区域，单击*添加*。

   此时将显示聚合对话框。
4. 选择一个或多个聚合。
5. 单击 **Add**。

   对话框已关闭，聚合显示在选定资源池的成员列表中。

从 **Active IQ Unified Manager** 的资源池中删除聚合

您可以从现有资源池中删除聚合：例如，当要将聚合用于其他目的时。

开始之前

您必须具有应用程序管理员或存储管理员角色。

仅当选择资源池时才会显示资源池成员。

步骤

1. 在左侧导航窗格中，单击 保护 > 资源池。
2. 选择要从中删除成员聚合的资源池。

   成员聚合列表显示在成员窗格中。
3. 选择一个或多个聚合。

   *移除*按钮已启用。
4. 单击 删除。

   此时将显示警告对话框。
5. 单击 **Yes** 继续。

选定的聚合将从“成员”窗格中删除。

删除 **Active IQ Unified Manager** 中的资源池

您可以在不再需要资源池时将其删除。例如，您可能希望将成员聚合从一个资源池重新分配到其他几个资源池，从而使原始资源池被废弃。

开始之前

您必须具有应用程序管理员或存储管理员角色。

仅当至少选择了一个资源池时，才会启用*删除*按钮。

步骤

1. 在左侧导航窗格中，单击 保护 > 资源池。
2. 选择要删除的资源池。
3. 单击 **Delete**。

   资源池将从资源池列表中删除，其聚合将从成员列表中删除。

监控 **Storage VM** 灾难恢复保护关系

了解 **Active IQ Unified Manager** 中的**Storage VM**灾难恢复关系

Active IQ Unified Manager 支持监控 Storage VM 灾难恢复关系，可在 Storage VM 级别的粒度上提供灾难恢复。Storage VM 灾难恢复可恢复 Storage VM 成员卷中的数据以及 Storage VM 配置。

从源 storage VM 到目标 storage VM 创建 storage VM DR 关系，以提供异步灾难恢复。您可以根据群集设置选择复制 storage VM 配置的全部或子集（不包括网络和协议配置）以及数据卷。

配置存储 VM 灾难恢复关系后，当源存储 VM 由于硬件故障或环境灾难而变得不可用时，将启动目标存储 VM，从而以最少的中断提供对数据的访问。同样，当源存储 VM 可用时，它会与目标存储 VM 重新同步，然后源重新启动以提供数据。您可以使用 SnapMirror 命令来配置和管理存储 VM 灾难恢复关系。

使用 **Active IQ Unified Manager** 中的关系页面监控存储 **VM**

您可以从“清单”的“保护”部分中的“关系”页面监控您的 storage VM 灾难恢复关系。默认情况下，“关系”页面仅列出顶级关系，因为应用了组成关系筛选器。

开始之前

您必须具有应用程序管理员或存储管理员角色。

您可以使用筛选器来查看 storage VM 灾难恢复关系。

步骤

1. 在左侧导航窗格中，单击*保护* > 关系。

   该页面显示所有类型的关系：卷、一致性组和存储 VM 关系。

2. 单击 筛选器，然后选择 关系对象类型 和 存储 **VM** 以仅查看存储 VM 灾难恢复关系。
3. 单击*应用过滤器*。

   您应该清除组成关系筛选器以查看所有保护关系。

   此页面仅显示 storage VM 灾难恢复关系。

从 **Active IQ Unified Manager** 的 **Storage VM** 页面查看保护关系

使用“存储虚拟机”页面，您可以查看现有存储虚拟机的灾难恢复关系状态。

开始之前

您必须具有应用程序管理员或存储管理员角色。

您还可以查看保护关系的详细信息，包括传输和滞后状态、源和目标详细信息。您可以按所需格式计划报告或下载现有报告。*显示/隐藏*按钮使您能够将所需列添加到报告中，因为它们默认情况下不会显示。

步骤

1. 在左侧导航窗格中，单击 存储 > 存储 **VM**。
2. 从*视图*菜单中，选择*关系* > 所有关系。

   “关系：所有关系”视图将与所有已配置的存储虚拟机一起显示。

在 **Active IQ Unified Manager** 中根据保护状态查看 **Storage VM**

您可以使用清单的存储虚拟机页面查看 Active IQ Unified Manager 中的所有存储虚拟机，并根据其保护状态筛选存储虚拟机。

开始之前

您必须具有应用程序管理员或存储管理员角色。

storage VMs 视图中添加了一个新列 Protection Role，用于提供有关 storage VM 是否受保护的信息。

如果源集群未添加到 Active IQ Unified Manager，则与该集群相关的所有信息在网格中不可用。

步骤

1. 在左侧导航窗格中，单击 存储 > 存储 **VM**。
2. 从*视图*菜单中，选择*运行状况* > 所有 **Storage VM**。

   此时将显示运行状况：所有 Storage VM。

3. 单击 筛选 可查看以下存储 VM 之一。

要查看	筛选值
受保护的 **storage VM**	保护角色*为*受保护
未受保护的 **Storage VM**	保护角色*为*未受保护

您不能同时查看受保护和未受保护的存储 VM。您需要清除现有筛选器才能重新应用新的筛选器选项。

4. 单击*应用过滤器*。

   未保存视图根据您的筛选器选择，显示受 storage VM 灾难恢复保护或未受 storage VM 灾难恢复保护的所有 storage VM。

在 **Active IQ Unified Manager** 中管理 **Storage VM** 关联

Storage virtual machine (storage VM) 关联是从源存储虚拟机到目标存储虚拟机的映射，合作伙伴应用程序将其用于资源选择和辅助卷配置。

无论目标 Storage VM 是辅助目标还是第三目标，都会在源 Storage VM 和目标 Storage VM 之间创建关联。您不能使用辅助目标 Storage VM 作为源来创建与第三目标 Storage VM 的关联。

作为应用程序管理员或存储管理员，您可以在 保护 > 存储 **VM** 关联 页面上查看环境中的存储 VM 关联。

您可以通过三种方式关联 SVM：

- 关联任何存储虚拟机：您可以在任何主源存储虚拟机和一个或多个目标 SVM 之间创建关联。这意味着当前需要保护的所有现有 SVM 以及未来创建的任何 SVM 都与指定的目标 SVM 相关联。例如，您可能希望将来自不同位置的多个不同来源的应用程序备份到一个位置中的一个或多个目标 SVM。
- 关联特定存储 **VM**：可以在特定源存储 VM 和一个或多个特定目标 SVM 之间创建关联。例如，如果要向许多客户端提供存储服务，而这些客户端的数据必须彼此独立，则可以选择此选项将特定源存储 VM 关联到仅分配给该客户端的特定目标存储 VM。
- 与外部存储虚拟机关联：您可以在源存储虚拟机与目标存储虚拟机的外部灵活卷之间创建关联。

创建存储 **VM** 关联

Create Storage Virtual Machine Associations 向导使合作伙伴保护应用程序能够将源存储虚拟机与目标存储虚拟机关联，以便与 SnapMirror 和 SnapVault 关系一起使用。合作伙伴应用程序在初始配置目标卷时使用这些关联来确定要选择哪些资源。dd

开始之前

- 您要关联的存储 VM 必须已存在。
- 您必须具有应用程序管理员或存储管理员角色。

对于任何源存储虚拟机和关系类型，您在每个目标集群上只能选择一个目标存储虚拟机。

使用“删除”和“创建”功能更改关联仅会影响将来的配置操作。它不会移动现有目标卷。

步骤

1. 在左侧导航窗格中，单击*保护* > 存储虚拟机关联。
2. 在 **Storage VM Associations** 页面上，单击 **Create**。

   *创建 Storage Virtual Machine 关联*向导已启动。

3. 选择以下源之一：
   - 任意

     如果要在任何主存储 VM 源与一个或多个目标存储 VM 之间创建关联，请选择此选项。这意味着当前需要保护的所有现有存储 VM 以及将来创建的任何存储 VM 都与指定的目标存储 VM 关联。例如，您可能希望将来自不同位置的多个不同源的应用程序备份到一个位置中的一个或多个目标存储 VM。

   - 单个

     如果要选择与一个或多个目标存储 VM 关联的特定源存储 VM，请选择此选项。例如，如果要向许多数据必须彼此分离的客户端提供存储服务，请选择此选项将特定存储 VM 源关联到仅分配给该客户端的特定存储 VM 目标。

   - 无（外部）

     如果要在源存储 VM 和目标存储 VM 的外部灵活卷之间创建关联，请选择此选项。

4. 选择要创建的一个或两个保护关系类型：
   - **SnapMirror**
   - **SnapVault**
5. 单击*下一步*。
6. 选择一个或多个 storage VM 保护目标。
7. 单击 **Finish**。

删除 **storage VM** 关联

您可以删除伙伴应用程序的存储虚拟机关联，以移除源和目标存储虚拟机之间的辅助配置关系；例如，当目标存储虚拟机已满并且您要创建新的存储虚拟机保护关联时，可以执行此操作。

开始之前

您必须具有应用程序管理员或存储管理员角色。

在至少选择一个存储 VM 关联之前，删除 按钮将被禁用。使用删除和创建功能更改关联仅影响未来的配置操作；它不会移动现有目标卷。

步骤

1. 在左侧导航窗格中，单击*保护* > 存储虚拟机关联。
2. 至少选择一个存储 VM 关联。

   *删除*按钮已启用。

3. 单击 **Delete**。

   此时将显示警告对话框。

4. 单击 **Yes** 继续。

   选定的 Storage VM 关联将从列表中删除。

支持 **Active IQ Unified Manager** 中存储服务的 **SVM** 和资源池要求

如果您遵守某些特定于存储服务的 SVM 关联和资源池要求，则可以更好地确保合作伙伴应用程序的一致性：例如，当您在 Unified Manager 中关联 SVM 并创建资源池，以支持由合作伙伴应用程序提供的存储服务中的保护拓扑时。

某些应用程序与 Unified Manager 服务器合作，提供自动在二级或三级位置的源卷和保护卷之间配置和执行 SnapMirror 或 SnapVault 备份保护的服务。要支持这些保护存储服务，必须使用 Unified Manager 配置必要的 SVM 关联和资源池。

要支持存储服务单跳或级联保护，包括从 SnapMirror 源或 SnapVault 主卷复制到目标 SnapMirror 或驻留在二级或三级位置的 SnapVault 备份卷，请遵守以下要求：

- 必须在包含 SnapMirror 源或 SnapVault 主卷的 SVM 与辅助卷或第三卷所在的任何 SVM 之间配置 SVM 关联。
  - 例如，要支持源卷 Vol_A 驻留在 SVM_1 上、SnapMirror 辅助目标卷 Vol_B 驻留在 SVM_2 上、第三 SnapVault 备份卷 Vol_ C 驻留在 SVM_3 上的保护拓扑，您必须使用 Unified Manager Web UI 配置 SVM_1 和 SVM_2 之间的 SnapMirror 关联以及 SVM_1 和 SVM_3 之间的 SnapVault 备份关联。

    在此示例中，SVM_2 和 SVM_3 之间的任何 SnapMirror 关联或 SnapVault 备份关联都是不必要的，并且不会使用。

  - 要支持源卷 Vol_A 和 SnapMirror 目标卷 Vol_B 都驻留在 SVM_1 上的保护拓扑，您必须配置 SVM_1 和 SVM_1 之间的 SnapMirror 关联。
- 资源池必须包括可用于关联 SVM 的集群聚合资源。

  您可以通过 Unified Manager Web UI 配置资源池，然后通过合作伙伴应用程序分配存储服务辅助目标和第三目标节点。

了解 **Active IQ Unified Manager** 中的作业

作业是可以使用 Unified Manager 监视的一系列任务。通过查看作业及其相关任务，您可以确定它们是否已成功完成。

当您创建 SnapMirror 和 SnapVault 关系时，当您执行任何关系操作（中断、编辑、静默、删除、恢复、重新同步和反向重新同步）时，当您执行数据还原任务时，当您登录到集群时等等，都会启动作业。

启动作业时，您可以使用“作业”页面和“作业详细信息”页面来监控作业以及相关作业任务的进度。

监控 **Active IQ Unified Manager** 中的作业

您可以使用“作业”页面来监视作业状态并查看作业属性，例如存储服务类型、状态、提交时间和完成时间，以确定作业是否已成功完成。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*保护* > 作业。

此时将显示作业页面。

2. 查看*状态*列以确定当前正在运行的那些作业的状态。
3. 单击作业名称可查看该特定作业的详细信息。

此时将显示作业详细信息页面。

在 **Active IQ Unified Manager** 中查看作业详细信息

启动作业后，您可以从“作业详细信息”页面跟踪其进度，并监视相关任务以发现可能的错误。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*保护* > 作业。
2. 在“作业”页面中，单击“名称”列中的作业名称，以显示与该作业关联的任务列表。
3. 单击任务，可在任务列表右侧的*任务详细信息*窗格和*任务消息*窗格中显示其他信息。

在 **Active IQ Unified Manager** 中中止作业

如果作业需要太长时间才能完成、遇到太多错误或不再需要，您可以使用“作业”页面中止该作业。只有当作业的状态和类型允许时，您才能中止作业。您可以中止任何正在运行的作业。

开始之前

您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*保护* > 作业。
2. 从作业列表中，选择一个作业，然后单击*中止*。
3. 在确认提示下，单击*是*以中止选定作业。

在 **Active IQ Unified Manager** 中重试失败的保护作业

采取措施修复失败的保护作业后，您可以使用 重试 再次运行该作业。重试作业将使用原始作业 ID 创建一个新作业。

开始之前

您必须具有应用程序管理员或存储管理员角色。

一次只能重试一个失败的作业。选择多个作业将禁用*重试*按钮。只能重试保护配置和保护关系操作类型的作业。

步骤

1. 在左侧导航窗格中，单击*保护* > 作业。
2. 从作业列表中，选择一个失败的保护配置或保护关系操作类型作业。

   *重试*按钮已启用。

3. 单击*重试*。

   作业已重新启动。

保护关系窗口和对话框说明

了解 **Active IQ Unified Manager** 中的资源池页面

“资源池”页面显示现有资源池及其成员，并使您能够创建、监控和管理资源池以进行配置。

命令按钮

这些命令按钮可用来执行下列任务：

- 创建

  启动“创建资源池”对话框，可用于创建资源池。

- 编辑

  使您能够编辑您创建的资源池的名称和说明。

- 删除

  用于删除一个或多个资源池。

资源池列表

“资源池”列表（以表格格式）显示现有资源池的属性。

- 资源池

  显示资源池的名称。

- 说明

  描述资源池。

- **SnapLock** 类型

  显示资源池中的聚合正在使用的 SnapLock 类型。SnapLock 类型的有效值为 Compliance、Enterprise 和 Non-SnapLock。一个资源池只能包含一种 SnapLock 类型的聚合。

- 总容量

显示资源池的总容量（以 MB、GB 等为单位）。

- 已用容量

  显示资源池中使用的空间量（以 MB、GB 等为单位）。

- 可用容量

  显示资源池中可用的空间量（以 MB、GB 等为单位）。

- 已用 **%**

  显示资源池中使用的空间百分比。

成员列表命令按钮

成员列表命令按钮可用于执行以下任务：

- 添加

  使您能够将成员添加到资源池。

- 删除

  用于从资源池中删除一个或多个成员。

成员列表

当选择资源池时，“成员”列表将（以表格形式）显示资源池成员及其属性。

- 状态

  显示成员聚合的当前状态。状态可以是 Critical（）、Error（）、Warning（）或 Normal（）。

- 聚合名称

  显示成员聚合的名称。

- **State**

  显示聚合的当前状态，可以是以下选项之一：

  - 脱机

    不允许读取或写入访问。

  - 联机

    允许对该聚合上托管的卷进行读取和写入访问。

  - 受限

允许进行有限的操作（例如奇偶校验重建），但不允许访问数据。

- 正在创建

  正在创建此聚合。

- 正在销毁

  此聚合正在被销毁。

- 失败

  聚合体无法联机。

- 已冻结

  此聚合（暂时）不为请求提供服务。

- 不一致

  聚合已被标记为已损坏；您应该与技术支持联系。

- 受 Iron 限制

  无法在聚合上运行诊断工具。

- 正在安装

  聚合正在挂载过程中。

- 部分

  至少为聚合找到了一个磁盘，但缺少两个或多个磁盘。

- 正在暂停

  此聚合正在静止。

- 已暂停

  聚合已静止。

- 已还原

  聚合还原已完成。

- 已卸载

  已卸载此聚合。

- 正在卸载

  此聚合正在脱机。

- 未知

  已发现聚合，但 Unified Manager 服务器尚未检索到聚合信息。

默认情况下，此列处于隐藏状态。

- 集群

  显示聚合所属的集群的名称。

- 节点

  显示聚合所在的节点的名称。

- 总容量

  显示聚合的总容量（以 MB、GB 等为单位）。

- 已用容量

  显示聚合中使用的空间量（以 MB、GB 等为单位）。

- 可用容量

  显示聚合中可用的空间量（以 MB、GB 等为单位）。

- 已用 **%**

  显示聚合中使用的空间百分比。

- 磁盘类型

  显示 RAID 配置类型，可为以下选项之一：

  - RAID0：所有 RAID 组的类型均为 RAID0。
  - RAID4：所有 RAID 组均为 RAID4 类型。
  - RAID-DP：所有 RAID 组的类型均为 RAID-DP。
  - RAID-TEC：所有 RAID 组的类型均为 RAID-TEC。
  - 混合 RAID：聚合包含不同 RAID 类型（RAID0、RAID4、RAID-DP 和 RAID-TEC）的 RAID 组。默认情况下，此列处于隐藏状态。

使用 **Active IQ Unified Manager** 中的 **Create Resource Pool** 对话框

您可以使用“创建资源池”对话框来命名和描述新资源池，以及向该资源池添加聚合和从该资源池删除聚合。

资源池名称

文本框使您可以添加以下信息以创建资源池：

使您能够指定资源池名称。

问题描述

用于描述资源池。

成员

显示资源池的成员。您还可以添加和删除成员。

命令按钮

这些命令按钮可用来执行下列任务：

- 添加

  打开“聚合”对话框，以便您可以将特定群集中的聚合添加到资源池。您可以添加来自不同群集的聚合，但不能将相同的聚合添加到多个资源池。

- 删除

  使您能够从资源池中移除选定的聚合。

- 创建

  创建资源池。在“资源池名称”或“描述”字段中输入信息之前，此按钮不会启用。

- 取消

  放弃更改并关闭“创建资源池”对话框。

使用 **Active IQ Unified Manager** 中的**"**编辑资源池**"**对话框

您可以使用“编辑资源池”对话框来更改现有资源池的名称和描述。例如，如果原始名称和描述不准确或不正确，您可以更改它们，使其更准确。

文本框

通过文本框可以更改选定资源池的以下信息：

- 资源池名称

  使您能够输入新名称。

- 说明

  使您能够输入新的描述。

命令按钮

这些命令按钮可用来执行下列任务：

- 保存

  保存对资源池名称和描述所做的更改。

- 取消

  放弃更改并关闭“编辑资源池”对话框。

使用 **Active IQ Unified Manager** 中的聚合对话框

可以使用“聚合”对话框选择要添加到资源池的聚合。

命令按钮

这些命令按钮可用来执行下列任务：

- 添加

  将所选聚合添加到资源池。在至少选择一个聚合之前，不会启用“添加”按钮。

- 取消

  放弃更改，并关闭“聚合”对话框。

聚合列表

“聚合”列表（以表格格式）显示受监控聚合的名称和属性。

- 状态

  显示卷的当前状态。状态可以是 Critical（）、Error（）、Warning（）或 Normal（）。

  可以将指针移到状态上，以查看有关为卷生成的一个或多个事件的详细信息。

- 聚合名称

  显示聚合的名称。

- **State**

  显示聚合的当前状态，可以是以下选项之一：

  - 脱机

    不允许读取或写入访问。

  - 受限

    允许进行有限的操作（例如奇偶校验重建），但不允许访问数据。

  - 联机

    允许对该聚合上托管的卷进行读取和写入访问。

- 正在创建

  正在创建此聚合。

- 正在销毁

  此聚合正在被销毁。

- 失败

  聚合体无法联机。

- 已冻结

  此聚合（暂时）不为请求提供服务。

- 不一致

  聚合已被标记为已损坏；您应该与技术支持联系。

- 受 Iron 限制

  无法在聚合上运行诊断工具。

- 正在安装

  聚合正在挂载过程中。

- 部分

  至少为聚合找到了一个磁盘，但缺少两个或多个磁盘。

- 正在暂停

  此聚合正在静止。

- 已暂停

  聚合已静止。

- 已还原

  聚合还原已完成。

- 已卸载

  此聚合已脱机。

- 正在卸载

  此聚合正在脱机。

- 未知

已发现聚合，但 Unified Manager 服务器尚未检索到聚合信息。

- 集群

  显示聚合所在的集群的名称。

- 节点

  显示包含聚合的存储控制器的名称。

- 总容量

  显示聚合的总数据大小（以 MB、GB 等为单位）。默认情况下，此列处于隐藏状态。

- 已提交的容量

  显示为聚合中的所有卷提交的总空间（以 MB、GB 等为单位）。默认情况下，此列是隐藏的。

- 已用容量

  显示聚合中使用的空间量（以 MB、GB 等为单位）。

- 可用容量

  显示可用于聚合中数据的空间量（以 MB、GB 等为单位）。默认情况下，此列处于隐藏状态。

- 可用 **%**

  显示聚合中可用于数据的空间百分比。默认情况下，此列是隐藏的。

- 已用 **%**

  显示聚合中数据使用的空间百分比。

- **RAID** 类型

  显示选定卷的 RAID 类型。RAID 类型可以是 RAID0、RAID4、RAID-DP、RAID-TEC 或混合 RAID。

了解 **Active IQ Unified Manager** 中的作业页面

通过“作业”页面，您可以查看当前正在运行的所有合作伙伴应用程序保护作业的当前状态和其他信息，以及已完成的作业。您可以使用此信息查看哪些作业仍在运行，以及作业是否成功或失败。

命令按钮

这些命令按钮可用来执行下列任务：

- 中止

  中止所选作业。此选项仅在所选作业正在运行时可用。

- 重试

  重新启动保护配置或保护关系操作类型的失败作业。一次只能重试一个失败的作业。如果选择了多个失败作业，则禁用*重试*按钮。无法重试失败的存储服务作业。

- 刷新

  刷新作业列表以及与其关联的信息。

作业列表

“作业”列表以表格形式显示正在进行的作业列表。默认情况下，该列表仅显示过去一周内生成的作业。您可以使用列排序和筛选来自定义要显示的作业。

- 状态

  显示作业的当前状态。状态可以是 Error （❗） 或 Normal （✅）。

- 作业 **ID**

  显示作业的标识号。默认情况下，此列处于隐藏状态。

  作业标识号是唯一的，由服务器在启动作业时分配。可以通过在列筛选器提供的文本框中输入作业标识号来搜索特定作业。

- 名称

  显示作业的名称。

- 类型

  显示作业类型。作业类型如下：

  - 集群采集

    Workflow Automation 作业正在重新发现集群。

  - 保护配置

    保护作业正在启动 Workflow Automation 工作流，例如 cron 计划、SnapMirror 策略创建等。

  - 保护关系操作

    保护作业正在运行 SnapMirror 操作。

  - 保护工作流链

    Workflow Automation 作业正在执行多个工作流。

  - 还原

    正在运行还原作业。

- 清理

  作业正在清理不再需要用于还原目的的存储服务成员项目。

- 符合

  作业正在检查存储服务成员的配置，以确保其符合要求。

- 销毁

  作业正在销毁存储服务。

- 导入

  作业正在将非托管存储对象导入现有存储服务。

- 修改

  该作业正在修改现有存储服务的属性。

- 订阅

  该作业正在为成员订阅存储服务。

- 取消订阅

  该作业正在从存储服务中取消订阅成员。

- 更新

  正在运行保护更新作业。

- **WFA** 配置

  Workflow Automation 作业正在推送群集凭据并同步数据库缓存。

- **State**

显示作业的运行状态。状态选项如下：

- 已中止

  此作业已中止。

- 中止

  作业正在中止。

- 已完成

  作业已完成。

- 运行中

作业正在运行。

- 提交时间

  显示作业提交时间。

- 持续时间

  显示作业完成所需的时间。默认情况下会显示此列。

- 完成时间

  显示作业完成的时间。默认情况下，此列处于隐藏状态。

了解 **Active IQ Unified Manager** 中的作业详细信息页面

作业详细信息页面使您能够查看有关正在运行、已排队或已完成的特定保护作业任务的状态和其他信息。您可以使用此信息来监控保护作业进度并排除作业故障。

作业摘要

作业摘要显示以下信息：

- 作业 ID
- 类型
- 州/省
- 提交时间
- 完成时间
- 持续时间

命令按钮

这些命令按钮可用来执行下列任务：

- 刷新

  刷新任务列表以及与每个任务关联的属性。

- 查看作业

  将您返回到“作业”页面。

作业任务列表

“作业任务”列表在表格中显示与特定作业关联的所有任务以及与每个任务相关的属性。

- 开始时间

  显示任务开始的日期和时间。默认情况下，最新任务将显示在列顶端，旧任务将显示在底端。

- 类型

  显示任务类型。

- **State**

  特定任务的状态：

  - 已完成

    任务已完成。

  - 已排队

    该任务即将运行。

  - 运行中

    任务正在运行。

  - 正在等待

    已提交作业，一些关联的任务正在等待排队和执行。

- 状态

  显示任务状态：

  - 错误（）

    任务失败。

  - 正常（）

    任务成功。

  - 已跳过（）

    任务失败，导致后续任务被跳过。

- 持续时间

  显示自任务开始以来的运行时间。

- 完成时间

  显示任务完成的时间。默认情况下，此列处于隐藏状态。

- 任务 **ID**

  显示标识作业的单个任务的 GUID。可以对该列进行排序和筛选。默认情况下，此列处于隐藏状态。

- 依赖关系顺序

显示一个表示图形中任务序列的整数，其中零被分配给第一个任务。默认情况下，此列处于隐藏状态。

- 任务详细信息窗格

  显示有关每个作业任务的其他信息，包括任务名称、任务描述以及（如果任务失败）失败的原因。

- 任务消息窗格

  显示特定于所选任务的消息。消息可能包含错误原因和解决建议。并非所有任务都显示任务消息。

使用 **Active IQ Unified Manager** 中的**"**高级二级设置**"**对话框

您可以使用“高级辅助设置”对话框在辅助卷上启用版本灵活的复制、多副本备份和与空间相关的设置。当您想要更改、启用或禁用当前设置时，可以使用“高级辅助设置”对话框。

空间相关设置会最大化存储的数据量，包括：重复数据删除、数据压缩、自动增长和空间保证。

对话框包括以下字段：

- 启用版本灵活的复制

  启用具有版本灵活复制功能的 SnapMirror。版本灵活的复制可实现对源卷的 SnapMirror 保护，即使目标卷运行的 ONTAP 版本早于源卷。

  - 启用备份

    如果启用了版本灵活的复制，则还可以将 SnapMirror 源数据的多个快照副本传输并保留在 SnapMirror 目标上。

- 启用重复数据删除

  在 SnapVault 关系中的辅助卷上启用重复数据删除，从而消除重复数据块以节省空间。当节省的空间至少为 10% 并且数据覆盖率不高时，您可以使用重复数据删除。重复数据删除通常用于虚拟化环境、文件共享和备份数据。默认情况下，此设置处于禁用状态。启用后，此操作将在每次传输后启动。

  - 启用数据压缩

    启用透明数据压缩。当节省的空间至少为 10% 时，当潜在的开销可以接受时，以及当有足够的系统资源在非高峰时段完成压缩时，您可以使用压缩。在 SnapVault 关系中，默认情况下会禁用此设置。仅当选择了重复数据删除时，压缩才可用。

  - 实时数据压缩

    通过在将数据写入磁盘之前压缩数据来实现即时的空间节省。当您的系统在高峰时段的利用率不超过 50%，并且系统可以在高峰时段容纳新的写入和额外的 CPU 时，您可以使用内联压缩。此设置仅在选择 “启用压缩” 时可用。

- 启用自动增长

  允许您在可用空间百分比低于指定阈值时自动扩展目标卷，前提是关联聚合中有可用空间。

- 最大大小

设置卷可以增长到的最大百分比。默认值为比源卷大小大 20%。如果当前大小大于或等于最大自动增长百分比，则卷不会自动增长。仅当启用了自动增长设置时，才会启用此字段。

- 增量大小

  指定在达到源卷的最大百分比之前，卷自动增长的百分比增量。

- 空间保证

  确保在辅助卷上分配足够的空间，以便数据传输始终成功。空间保障设置可为以下选项之一：

  - 文件
  - 卷
  - 无 + 例如，您可能有一个 200 GB 的卷，其中包含总共 50 GB 的文件；但是，这些文件仅包含 10 GB 的数据。无论源上的内容如何，卷保证都会将 200 GB 分配给目标卷。文件保证分配 50 GB，以确保为源上的文件保留足够的空间；在这种情况下，选择“无”意味着在目标上仅为源上文件数据使用的实际空间分配 10 GB。

默认情况下，空间保证设置为 Volume。

命令按钮

这些命令按钮可用来执行下列任务：

- 应用

  保存选定的效率设置，并在“配置保护”对话框中单击 应用 时应用它们。

- 取消

  放弃您的选择并关闭“高级目标设置”对话框。

使用 **Active IQ Unified Manager** 中的 **Advanced Destination Settings** 对话框

您可以使用“高级目标设置”对话框在目标卷上启用空间保证设置。当源上禁用了空间保证，但您希望在目标上启用它时，您可以选择高级设置。SnapMirror 关系中的重复数据删除、压缩和自动增长设置继承自源卷，且无法更改。

空间保证

确保在目标卷上分配足够的空间，以便数据传输始终成功。空间保障设置可为以下选项之一：

- 文件
- 卷
- 无

例如，您可能有一个 200 GB 的卷，其中包含总共 50 GB 的文件；但是，这些文件仅包含 10 GB 的数据。无论源上的内容如何，卷保证都会将 200 GB 分配给目标卷。文件保证分配 50 GB，以确保在目标上为源文件保留足够的空间；在这种情况下选择 无 意味着在目标上仅为源上的文件数据所使用的实际空间分配 10 GB。

默认情况下，空间保证设置为 Volume。

使用 **Active IQ Unified Manager** 中的还原对话框

您可以使用“还原”对话框从特定 Snapshot 副本将数据还原到卷。

还原自

通过“还原来源”区域，可以指定要从何处还原数据。

- 卷

  指定要从中还原数据的卷。默认情况下，将选择启动还原操作的卷。您可以从下拉列表中选择一个不同的卷，该列表包含与启动还原操作的卷具有保护关系的所有卷。

- **Snapshot** 副本

  指定要用于还原数据的 Snapshot 副本。默认情况下，将选择最新的 Snapshot 副本。您还可以从下拉列表中选择其他 Snapshot 副本。Snapshot 副本列表会根据所选的卷而变化。

- 列出最多 **995** 个文件和目录

  默认情况下，列表中最多显示 995 个对象。如果要查看所选卷中的所有对象，可以取消选中此复选框。如果项目数量非常大，此操作可能需要一些时间。

选择要还原的项

选择要还原的项目区域允许您选择要还原的整个卷或特定文件和文件夹。最多可以选择 10 个文件、文件夹或两者的组合。当选择的项目数量达到上限时，项目选择复选框将被禁用。

- 路径字段

  显示要还原的数据的路径。您可以导航到要还原的文件夹和文件，也可以键入路径。在您选择或键入路径之前，此字段为空。选择路径后，单击  将使您在目录结构中向上移动一个级别。

- 文件夹和文件列表

  显示输入路径的内容。默认情况下，最初将显示根文件夹。单击文件夹名称将显示文件夹的内容。

您可以按以下方式选择要还原的项：

- 当您在路径字段中输入指定了特定文件名的路径时，指定的文件将显示在“文件夹和文件”中。
- 输入路径而不指定特定文件时，文件夹的内容将显示在“文件夹和文件”列表中，您可以选择最多 10 个文件、文件夹或两者的组合进行还原。

  如果文件夹包含 995 个以上的项，则会显示一条消息，指示要显示的项过多，如果继续此操作，则将还原指定文件夹中的所有项。如果要查看所选卷中的所有对象，可以取消选中 “最多列出 995 个文件和目录” 复选框。



您不能还原 NTFS 文件流。

还原至

通过“还原到”区域，您可以指定要还原数据的位置。

- **Volume_Name** 中的原始位置

  将所选数据还原到最初备份数据的源目录。

- 备用位置

  将所选数据还原到一个新位置：

  - 还原路径

    指定还原所选数据的替代路径。路径必须已存在。您可以使用 **Browse** 按钮导航到要还原数据的位置，也可以使用以下格式手动输入路径 `cluster://svm/volume/path`。

  - 保留目录层次结构

    选中后，保留原始文件或目录的结构。例如，如果源是 /A/B/C/myFile.txt，目标是 /X/Y/Z，则 Unified Manager 使用目标上的以下目录结构还原数据：/X/Y/Z/A/B/C/myFile.txt。

命令按钮

这些命令按钮可用来执行下列任务：

- 取消

  放弃选择并关闭“还原”对话框。

- 还原

  应用您的选择并开始还原过程。

使用 **Active IQ Unified Manager** 中的**"**浏览目录**"**对话框

当您想要将数据还原到与原始源不同的集群和 SVM 上的目录时，可以使用“浏览目录”对话框。默认情况下会选择原始源集群和卷。

通过“浏览目录”对话框，您可以选择要将数据还原到的集群、SVM、卷和目录路径。

- 集群

  列出可以还原的可用群集目标。默认情况下，将选择初始源卷的群集。

- **SVM** 下拉列表

  列出可用于选定集群的可用 SVM。默认情况下，将选择原始源卷的 SVM。

- 卷

  列出所选 SVM 中的所有读/写卷。您可以按名称和可用空间筛选卷。空间最多的卷将列在首位，依此类推，按降序排列。默认情况下，将选择原始源卷。

- 文件路径文本框

  使您能够键入要将数据还原到的文件路径。您输入的路径必须已存在。

- 名称

  显示所选卷的可用文件夹的名称。单击名称列表中的文件夹将显示子文件夹（如果有）。不显示文件夹中包含的文件。选择文件夹后，单击  可在目录结构中向上移动一级。

命令按钮

这些命令按钮可用来执行下列任务：

- 选择目录

  应用您的选择并关闭“浏览目录”对话框。如果未选择目录，则禁用此按钮。

- 取消

  放弃您的选择并关闭“浏览目录”对话框。

使用 **Active IQ Unified Manager** 中的**"**配置保护**"**对话框

您可以使用“配置保护”对话框为集群上的所有读取、写入和数据保护卷创建 SnapMirror 和 SnapVault 关系，以确保复制源卷或主卷上的数据。

源选项卡

- 拓扑视图

  显示要创建的关系的可视化表示。默认情况下，突出显示拓扑中的源。

- 源信息

  显示有关所选源卷的详细信息，包括以下信息：

  - 源集群名称
  - 源 SVM 名称
  - 累计卷总大小

    显示所选所有源卷的总大小。

  - 累计卷使用大小

    显示所有选定源卷的累计已用卷大小。

  - 源卷

    在表中显示以下信息：

- 源卷

  显示选定源卷的名称。

- 类型

  显示卷类型。

- SnapLock 类型

  显示卷的 SnapLock 类型。选项包括合规、企业和非 SnapLock。

- Snapshot 副本

  显示用于基线传输的 Snapshot 副本。如果源卷为读/写，则 Snapshot copy 列中的 Default 值表示默认情况下会创建新的 Snapshot 副本，并用于基线传输。如果源卷是数据保护卷，则 Snapshot copy 列中的 Default 值表示未创建新的 Snapshot 副本，并且所有现有 Snapshot 副本都将传输到目标。单击 Snapshot 副本值将显示 Snapshot 副本列表，您可以从中选择要用于基线传输的现有 Snapshot 副本。如果源类型为数据保护，则无法选择其他默认 Snapshot 副本。

SnapMirror 选项卡

使您能够在创建 SnapMirror 关系时，为保护关系指定目标集群、存储虚拟机 (SVM) 和聚合，以及目标的命名约定。您还可以指定 SnapMirror 策略和计划。

- 拓扑视图

  显示您正在创建的关系的可视化表示。默认情况下，拓扑中的 SnapMirror 目标资源会突出显示。

- 目标信息

  使您能够为保护关系选择目标资源：

  - 高级链接

    在创建 SnapMirror 关系时启动“高级目标设置”对话框。

  - 集群

    列出可用作保护目标主机的群集。此字段为必填项。

  - 存储虚拟机 (SVM)

    列出选定集群上可用的 SVM。在填充 SVM 列表之前，必须选择集群。此字段必填。

  - 聚合

    列出选定 SVM 上可用的聚合。在填充聚合列表之前，必须选择一个集群。此字段必填。聚合列表显示以下信息：

    - 排名

      当多个聚合满足目标的所有要求时，根据以下条件，排名表示列出聚合的优先级：

A. 首选位于与源卷节点不同的节点上的聚合，以实现故障域分离。

B. 首选卷较少的节点上的聚合，以便在集群中的节点之间实现负载均衡。

C. 为了实现容量平衡，首选可用空间多于其他聚合的聚合。排名为 1 表示根据这三个标准，该聚合是最优选的。

- 聚合名称

  聚合的名称

- 可用容量
- 聚合上可用于数据的空间量
- 资源池

  聚合所属的资源池的名称

◦ 命名约定

指定应用于目标卷的默认命名约定。您可以接受所提供的命名约定，也可以创建自定义约定。命名约定可以具有以下属性：%C、%M、%V 和 %N，其中 %C 是集群名称，%M 是 SVM 名称，%V 是源卷，%N 是拓扑目标节点名称。

如果您的输入无效，命名约定字段将以红色突出显示。单击 “Preview Name” 链接将显示您输入的命名约定的预览，并且当您在文本字段中键入命名约定时，预览文本会动态更新。创建关系时，系统会将 001 到 999 之间的后缀附加到目标名称，以替换预览文本中显示的 nnn，其中首先分配 001，其次分配 002，依此类推。

- 关系设置

使您能够指定保护关系使用的最大传输速率、SnapMirror 策略和计划：

◦ 最大传输速率

指定通过网络在集群之间传输数据的最大速率。如果选择不使用最大传输速率，则关系之间的基线传输将不受限制。

◦ SnapMirror 策略

为关系指定 ONTAP SnapMirror 策略。默认值为 DPDefault。

◦ 创建策略

启动“创建 SnapMirror 策略”对话框，可使用此对话框创建和使用新 SnapMirror 策略。

◦ SnapMirror 计划

指定关系的 ONTAP SnapMirror 策略。可用的计划包括 None、5min、8hour、daily、hourly 和 weekly。默认值为 None，表示没有计划与此关系关联。没有计划的关系没有滞后状态值，除非它们属于存储服务。

◦ 创建计划

启动“创建计划”对话框，可使用此对话框创建新 SnapMirror 计划。

SnapVault 选项卡

使您能够在创建 SnapVault 关系时为保护关系指定辅助集群、SVM 和聚合，以及辅助卷的命名约定。您还可以指定 SnapVault 策略和计划。

- 拓扑视图

  显示要创建的关系的可视化表示。默认情况下，拓扑中的 SnapVault 辅助资源会突出显示。

- 二级信息

  使您能够为保护关系选择二级资源：

  - 高级链接

    启动“高级辅助设置”对话框。

  - 集群

    列出可用作辅助保护主机的群集。此字段为必填项。

  - 存储虚拟机 (SVM)

    列出选定集群上可用的 SVM。在填充 SVM 列表之前，必须选择集群。此字段必填。

  - 聚合

    列出选定 SVM 上可用的聚合。在填充聚合列表之前，必须选择一个集群。此字段必填。聚合列表显示以下信息：

    - 排名

      当多个聚合满足目标的所有要求时，根据以下条件，排名表示列出聚合的优先级：

      A. 首选位于与主卷节点不同的节点上的聚合，以实现故障域分离。
      B. 首选卷较少的节点上的聚合，以便在集群中的节点之间实现负载均衡。
      C. 为了实现容量平衡，首选可用空间多于其他聚合的聚合。排名为 1 表示根据这三个标准，该聚合是最优选的。

    - 聚合名称

      聚合的名称

    - 可用容量
    - 聚合上可用于数据的空间量
    - 资源池

      聚合所属的资源池的名称

- 命名约定

  指定应用于辅助卷的默认命名约定。您可以接受提供的命名约定，也可以创建自定义约定。命名约定可以具有以下属性：%C、%M、%V 和 %N，其中 %C 是集群名称，%M 是 SVM 名称，%V 是源卷，%N 是拓扑辅助节点名称。

如果您的输入无效，命名约定字段将以红色突出显示。单击 “Preview Name” 链接将显示您输入的命名约定的预览，并且当您在文本字段中键入命名约定时，预览文本会动态更新。如果键入无效值，无效信息将在预览区域中显示为红色问号。创建关系时，会将 001 到 999 之间的后缀附加到辅助名称中，以替换预览文本中显示的 nnn，其中首先分配 001，其次分配 002，依此类推。

- 关系设置

  使您能够指定保护关系使用的最大传输速率、SnapVault 策略和 SnapVault 计划：

  - 最大传输速率

    指定通过网络在集群之间传输数据的最大速率。如果选择不使用最大传输速率，则关系之间的基线传输将不受限制。

  - SnapVault 策略

    为关系指定 ONTAP SnapVault 策略。默认值为 XDPDefault。

  - 创建策略

    启动“创建 SnapVault 策略”对话框，可使用此对话框创建和使用新的 SnapVault 策略。

  - SnapVault 计划

    指定关系的 ONTAP SnapVault 计划。可用计划包括 None、5min、8hour、daily、hourly 和 weekly。默认值为 None，表示没有计划与此关系关联。没有计划的关系没有滞后状态值，除非它们属于存储服务。

  - 创建计划

    启动“创建计划”对话框，可使用此对话框创建 SnapVault 计划。

命令按钮

这些命令按钮可用来执行下列任务：

- 取消

  放弃选择并关闭“配置保护”对话框。

- 应用

  应用所选内容并开始保护过程。

使用 **Active IQ Unified Manager** 中的**"**创建计划**"**对话框

“创建计划”对话框可用于为 SnapMirror 和 SnapVault 关系传输创建基本或高级保护计划。

由于数据频繁更新，您可以创建新计划以增加数据传输频率，也可以在数据不经常更改时创建不太频繁的计划。

无法为 SnapMirror 同步关系配置计划。

- 目标集群

  您在“配置保护”对话框的 SnapVault 选项卡或 SnapMirror 选项卡中选择的集群名称。

- 计划名称

  您为计划提供的名称。计划名称可以由字符 A 至 Z、a 至 z、0 至 9 以及以下任意特殊字符组成：! @ # $ % ^ & * ( ) _ -。计划名称不得包含以下字符：< >。

- 基本或高级

  要使用的计划模式。

  基本模式包括以下元素：

  - 重复

    计划传输发生的频率。选项包括每小时、每天和每周。

  - 天

    当选择每周重复时，传输发生的星期几。

  - 时间

    当选择“每日”或“每周”时，发生传输的时间。

    高级模式包括以下元素：

  - 个月

    表示一年中月份的逗号分隔的数字列表。有效值为 0 到 11，零表示 1 月，依此类推。此元素是可选的。将字段留空意味着每个月都会发生传输。

  - 天

    以逗号分隔的数字列表，表示每月的某一天。有效值为 1 到 31。此元素是可选的。将该字段留空意味着每月的每一天都会发生传输。

  - 工作日

    一个以逗号分隔的数字列表，表示一周中的几天。有效值为 0 到 6，其中 0 表示星期日，依此类推。此元素是可选的。将该字段留空意味着一周中的每一天都会进行传输。如果指定了一周中的某一天，但未指定一个月中的某一天，则仅在指定的一周中的某一天进行传输，而不是每天进行传输。

  - 小时

    以逗号分隔的数字列表，表示一天中的小时数。有效值为 0 至 23，0 表示午夜。此元素是可选的。

- 分钟

  一个以逗号分隔的数字列表，表示一小时内的分钟数。有效值为 0 到 59。此元素是必需的。

在 **Active IQ Unified Manager** 中使用“创建 **SnapMirror** 策略”对话框

“创建 SnapMirror 策略”对话框使您能够创建策略，以设置 SnapMirror 传输的优先级。您可以使用策略来最大限度地提高从源到目的地的传输效率。

- 目标集群

  您在“配置保护”对话框的 SnapMirror 选项卡中选择的集群名称。

- 目标 **SVM**

  在“配置保护”对话框 SnapMirror 选项卡中选择的 SVM 名称。

- **Policy Name**

  您为新策略提供的名称。策略名称可以由字符 A 到 Z、a 到 z、0 到 9、句点（.）、连字符（-）和下划线（_）组成。

- 传输优先级

  异步操作的传输运行优先级。您可以选择“正常”或“低”。具有指定正常传输优先级的策略的传输关系，会在具有指定低传输优先级的策略的传输关系之前运行。

- **Comment**

  您可以在其中添加有关策略的注释的可选字段。

- 传输重新启动

  指示在传输被中止操作或任何类型的故障（如网络中断）中断时应采取的重新启动操作。您可以从以下选项中选择一项：

  - 始终

    指定在重新启动传输之前创建新 Snapshot 副本，然后（如果存在）从检查点重新启动传输，然后从新创建的 Snapshot 副本进行增量传输。

  - 从不

    指定从不重新启动中断的传输。

命令按钮

这些命令按钮可用来执行下列任务：

- 取消

  放弃选择并关闭“配置保护”对话框。

- 应用

  应用您的选择并开始保护过程。

在 **Active IQ Unified Manager** 中使用“创建 **SnapVault** 策略”对话框

可使用“创建 SnapVault 策略”对话框创建策略以设置 SnapVault 传输的优先级。可使用策略最大限度地提高从主卷到辅助卷的传输效率。

- 目标集群

  您在“配置保护”对话框的 SnapVault 选项卡中选择的集群名称。

- 目标 **SVM**

  在“配置保护”对话框的 SnapVault 选项卡中选择的 SVM 名称。

- **Policy Name**

  您为新策略提供的名称。策略名称可以由字符 A 到 Z、a 到 z、0 到 9、句点（.）、连字符（-）和下划线（_）组成。

- 传输优先级

  传输运行的优先级。您可以选择“正常”或“低”。具有指定正常传输优先级策略的传输关系会在具有指定低传输优先级策略的传输关系之前运行。默认设置为“正常”。

- **Comment**

  一个可选字段，您可以在其中添加最多 255 个字符的有关 SnapVault 策略的注释。

- 忽略访问时间

  指定对于仅更改了访问时间的文件，是否忽略增量传输。

- 复制标签

  在表格中列出与 ONTAP 选择的 Snapshot 副本关联的规则，这些副本在策略中具有特定的复制标签。还提供以下信息和操作：

  - 命令按钮

    通过命令按钮，您可以执行以下操作：

    - 添加

      使您能够创建 Snapshot 副本标签和保留计数。

    - 编辑保留数量

      使您能够更改现有 Snapshot 副本标签的保留计数。保留计数必须为介于 1 到 251 之间的数字。所有规则的所有保留计数之和不得超过 251。

- 删除

  使您能够删除现有 Snapshot 副本标签。

- Snapshot 副本标签

  显示 Snapshot 副本标签。如果选择具有相同本地 Snapshot 副本策略的一个或多个卷，则会显示该策略中每个标签的条目。如果选择具有两个或多个本地 Snapshot 副本策略的多个卷，则该表将显示所有策略中的所有标签

- 计划

  显示与每个 Snapshot 副本标签关联的计划。如果一个标签有多个与其关联的计划，则该标签的计划将以逗号分隔的列表显示。如果选择具有相同标签但具有不同计划的多个卷，计划将显示 “Various”，以指示多个计划与所选卷相关联。

- 目标保留数量

  显示在 SnapVault 辅助上保留的具有指定标签的 Snapshot 副本数。具有多个计划的标签的保留计数显示每个标签和计划对的保留计数总和。如果选择具有两个或多个本地 Snapshot 副本策略的多个卷，则保留计数为空。

在 **Active IQ Unified Manager** 中编辑保护关系

您可以编辑现有的保护关系，以更改最大传输速率、保护策略或保护计划。

目标卷信息

- 目标集群

  所选目标集群的名称。

- 目标 **SVM**

  所选 SVM 的名称

- 关系设置

  使您能够指定保护关系使用的最大传输速率、SnapMirror 策略和计划：

  - 最大传输速率

    指定通过网络在群集之间传输基线数据的最大速率。选中后，网络带宽将限制为您指定的值。您可以输入一个数值，然后选择千字节/秒（KBps）、兆字节/秒（MBps）、吉字节/秒（GBps）或太字节/秒（TBps）。指定的最大传输速率必须大于 1 KBps 且小于 4 TBps。如果选择不使用最大传输速率，则关系之间的基线传输是无限的。如果主群集和辅助群集相同，则禁用此设置。

  - SnapMirror 策略

    为关系指定 ONTAP SnapMirror 策略。默认值为 DPDefault。

  - 创建策略

启动“创建 SnapMirror 策略”对话框，可使用此对话框创建和使用新 SnapMirror 策略。

- SnapMirror 计划

  指定关系的 ONTAP SnapMirror 策略。可用的计划包括 None、5min、8hour、daily、hourly 和 weekly。默认值为 None，表示没有计划与此关系关联。没有计划的关系没有滞后状态值，除非它们属于存储服务。

- 创建计划

  启动“创建计划”对话框，可使用此对话框创建新 SnapMirror 计划。

命令按钮

这些命令按钮可用来执行下列任务：

- 取消

  放弃选择并关闭“配置保护”对话框。

- 提交

  应用您的选择并关闭“编辑关系”对话框。

使用 **Active IQ Unified Manager** 中的 **Initialize/Update** 对话框

初始化/更新对话框使您能够对新保护关系执行首次基线传输，或者在关系已初始化且您希望执行手动、非计划性增量更新时更新该关系。

传输选项选项卡

通过“传输选项”选项卡，您可以更改传输的初始化优先级并更改传输期间使用的带宽。

- 传输优先级

  运行传输的优先级。您可以选择“正常”或“低”。具有指定正常传输优先级的策略的关系在指定低传输优先级的策略之前运行。默认情况下选择正常。

- 最大传输速率

  指定通过网络在群集之间传输数据的最大速率。如果选择不使用最大传输速率，则关系之间的基线传输不受限制。如果选择多个具有不同最大传输速率的关系，则可以指定以下最大传输速率设置之一：

  - 使用设置或编辑各个关系期间指定的值

    选中后，初始化和更新操作将使用每个关系创建或编辑时指定的最大传输速率。此字段仅在初始化或更新具有不同传输速率的多个关系时可用。

  - 无限制

    表示关系之间的传输没有带宽限制。此字段仅在初始化或更新具有不同传输速率的多个关系时可用。

- 将带宽限制为

  选中后，网络带宽将限制为您指定的值。您可以输入一个数值，然后选择千字节/秒（KBps）、兆字节/秒（MBps）、千兆字节/秒（GBps）或太字节/秒（TBps）。您指定的最大传输速率必须大于 1 KBps 且小于 4 TBps。

源 **Snapshot** 副本选项卡

“源 Snapshot 副本”选项卡将显示有关用于基线传输的源 Snapshot 副本的以下信息：

- 源卷

  显示相应源卷的名称。

- 目标卷

  显示选定目标卷的名称。

- 源类型

  显示卷类型。类型可以是读/写或数据保护。

- **Snapshot** 副本

  显示用于数据传输的 Snapshot 副本。单击 Snapshot 副本值将显示“选择源 Snapshot 副本”对话框，您可以在其中为传输选择特定的 Snapshot 副本，具体取决于您拥有的保护关系类型和正在执行的操作。指定其他 Snapshot 副本的选项不适用于数据保护类型源。

命令按钮

这些命令按钮可用来执行下列任务：

- 取消

  放弃您的选择并关闭“初始化/更新”对话框。

- 提交

  保存选择并启动初始化或更新作业。

使用 **Active IQ Unified Manager** 中的重新同步对话框

通过“重新同步”对话框，您可以重新同步先前已中断且目标已变为读/写卷的 SnapMirror 或 SnapVault 关系上的数据。当源卷上所需的通用 Snapshot 副本被删除，导致 SnapMirror 或 SnapVault 更新失败时，您也可以执行重新同步。

重新同步选项选项卡

“重新同步选项”选项卡用于设置要重新同步的保护关系的传输优先级和最大传输速率。

- 传输优先级

运行传输的优先级。您可以选择“正常”或“低”。具有指定正常传输优先级的策略的关系会在具有指定低传输优先级的策略的关系之前运行。

- 最大传输速率

  指定通过网络在集群之间传输数据的最大速率。选中后，网络带宽将限制为您指定的值。您可以输入一个数值，然后选择千字节/秒（KBps）、兆字节/秒（MBps）、千兆字节/秒（GBps）或 TBps。如果选择不使用最大传输速率，则关系之间的基线传输不受限制。

源 **Snapshot** 副本选项卡

“源 Snapshot 副本”选项卡将显示有关用于基线传输的源 Snapshot 副本的以下信息：

- 源卷

  显示相应源卷的名称。

- 目标卷

  显示选定目标卷的名称。

- 源类型

  显示卷类型：读/写或数据保护。

- **Snapshot** 副本

  显示用于数据传输的快照副本。单击“快照副本”值将显示“选择源快照副本”对话框，其中可以选择传输的特定快照副本，具体取决于您拥有的保护关系类型和正在执行的操作。

命令按钮

- 提交

  开始重新同步过程并关闭“重新同步”对话框。

- 取消

  取消选择并关闭“重新同步”对话框。

使用 **Active IQ Unified Manager** 中的 **Select Source Snapshot Copy** 对话框

您可以使用“选择源 Snapshot 副本”对话框选择特定的 Snapshot 副本以在保护关系之间传输数据，或者选择默认行为，该默认行为取决于您是初始化、更新还是重新同步关系，以及关系是否为 SnapMirror 或 SnapVault。

默认

使您能够选择默认行为，以确定将哪个 Snapshot 副本用于 SnapVault 和 SnapMirror 关系的初始化、更新和重新同步传输。

如果执行 SnapVault 传输，则每个操作的默认行为如下：

操作	当源为读/写时的默认 **SnapVault** 行为	源为数据保护 **(DP)** 时的默认 **SnapVault** 行为
初始化	创建新的 Snapshot 副本并将其传输。	传输上次导出的 Snapshot 副本。
更新	仅传输策略中指定的标记的 Snapshot 副本。	传输上次导出的 Snapshot 副本。
重新同步	传输在最新通用 Snapshot 副本之后创建的所有标记 Snapshot 副本。	传输最新的带标签 Snapshot 副本。

如果执行 SnapMirror 传输，则每个操作的默认行为如下：

操作	默认 **SnapMirror** 行为	默认 **SnapMirror** 行为（当关系是 **SnapMirror** 到 **SnapMirror** 级联中的第二个跃点时）
初始化	创建一个新 Snapshot 副本，并传输该副本以及在该新 Snapshot 副本之前创建的所有 Snapshot 副本。	从源传输所有 Snapshot 副本。
更新	创建一个新 Snapshot 副本，并传输该副本以及在该新 Snapshot 副本之前创建的所有 Snapshot 副本。	传输所有 Snapshot 副本。
重新同步	创建一个新 Snapshot 副本，然后从源传输所有 Snapshot 副本。	将所有 Snapshot 副本从辅助卷传输到第三卷，并删除创建最新通用 Snapshot 副本后添加的所有数据。

现有 **Snapshot** 副本

如果该操作允许选择 Snapshot 副本，则可从列表中选择现有的 Snapshot 副本。

- **Snapshot** 副本

  显示可以从中选择进行传输的现有 Snapshot 副本。

- 创建日期

  显示创建 Snapshot 副本的日期和时间。Snapshot 副本按从最新到最旧的顺序列出，最新的位于列表顶部。

如果您正在执行 SnapVault 传输，并且要选择要从源传输到目标的现有 Snapshot 副本，则每个操作的行为如下：

操作	指定 **Snapshot** 副本时的 **SnapVault** 行为	在级联中指定 **Snapshot** 副本时的 **SnapVault** 行为
初始化	传输指定的 Snapshot 副本。	数据保护卷不支持选择源 Snapshot 副本。
更新	传输指定的 Snapshot 副本。	数据保护卷不支持选择源 Snapshot 副本。
重新同步	传输选定的 Snapshot 副本。	数据保护卷不支持选择源 Snapshot 副本。

如果您正在执行 SnapMirror 传输，并且要选择现有的 Snapshot 副本从源传输到目标，则每个操作的行为如下：

操作	指定 **Snapshot** 副本时的 **SnapMirror** 行为	在级联中指定 **Snapshot** 副本时的 **SnapMirror** 行为
初始化	传输源上的所有 Snapshot 副本，直到指定的 Snapshot 副本。	数据保护卷不支持选择源 Snapshot 副本。
更新	传输源上的所有 Snapshot 副本，直到指定的 Snapshot 副本。	数据保护卷不支持选择源 Snapshot 副本。
重新同步	从源传输所有 Snapshot 副本，直到选定的 Snapshot 副本，然后删除创建最新通用 Snapshot 副本后添加的所有数据。	数据保护卷不支持选择源 Snapshot 副本。

命令按钮

这些命令按钮可用来执行下列任务：

- 提交

  提交选择并关闭“选择源 Snapshot 副本”对话框。

- 取消

  放弃选择并关闭“选择源 Snapshot 副本”对话框。

在 **Active IQ Unified Manager** 中反向重新同步

如果由于源卷被禁用而导致保护关系中断，并且目标卷被设置为读/写卷，则反向重新同步将使您能够反转关系方向，从而使目标卷成为新的源卷，并且源卷将成为新的目标卷。

当灾难导致保护关系中的源卷不可用时，您可以将目标卷转换为读/写模式来提供数据，同时修复或更换源、更新源并重新建立关系。当您执行反向重新同步操作时，源上比通用 Snapshot 副本上的数据更新的数据将被删除。

反向重新同步之前

在反向重新同步操作之前显示关系的源和目标。

- 源卷

  反向重新同步操作之前的源卷的名称和位置。

- 目标卷

  反向重新同步操作之前目标卷的名称和位置。

反向重新同步之后

显示保留重新同步操作后关系的源和目标。

- 源卷

  反向重新同步操作后源卷的名称和位置。

- 目标卷

  反向重新同步操作后目标卷的名称和位置。

命令按钮

通过命令按钮，您可以执行以下操作：

- 提交

  开始反向重新同步过程。

- 取消

  关闭“反向重新同步”对话框，而不启动反向重新同步操作。

在 **Active IQ Unified Manager** 中显示"关系：所有关系"视图

“关系：所有关系”视图显示有关存储系统上的保护关系的信息。

默认情况下，当您访问“关系”页面时，显示的报告将包括卷和存储 VM 的顶级保护关系。页面顶端的控件使您能够选择特定视图、执行搜索以查找特定对象、创建和应用筛选器以缩小显示数据的列表、在页面上添加/删除/重新排序列以及将页面上的数据导出为 .csv、.pdf 或 .xlsx 文件。自定义页面后，您可以将结果保存为自定义视图，然后计划定期生成此数据的报告并通过电子邮件发送。默认情况下，当您选择 关系 菜单时，显示的报告包括数据中心中卷和存储 VM 的保护关系。您可以使用 筛选器 选项仅查看选定的存储系统，如仅查看卷或仅查看存储 VM。相同的报告显示在“存储”页面中，仅适用于选定的存储实体。如果要查看卷或存储 VM 关系，可以访问 存储 > 卷 > 关系：所有关系 页面或访问 保护 > 关系 > 关系：所有关系，然后使用 筛选器 中的 关系对象类型 选项仅过滤卷或存储 VM 数据。

"关系"页面列出了所有保护关系，其中包含目标集群的 **View in System Manager** 链接，可用于在 ONTAP System Manager 中查看相同的对象。

- 状态

  显示保护关系的当前状态。

  状态可以是错误（）、警告（）或正常（）之一。

- 源 **Storage VM**

  显示源 SVM 的名称。您可以通过单击 SVM 名称来查看有关源 SVM 的更多详细信息。

  当集群上存在 SVM 但尚未添加到 Unified Manager 清单中时，或者该 SVM 是在集群上次刷新后创建时，此字段将为空。您必须确保 SVM 存在，或者对集群执行重新发现以刷新资源列表。

- 源

  根据您的选择显示受保护的源卷或源存储 VM。您可以通过单击卷或存储 VM 名称来查看有关源卷或存储 VM 的更多详细信息。

如果显示消息 `Resource-key not discovered`，这可能表示该卷存在于集群上但尚未添加到 Unified Manager 清单中，或者该卷是在集群上次刷新后创建的。您必须确保卷存在，或在集群上执行重新发现以刷新资源列表。

- 目标 **Storage VM**

  显示目标 SVM 的名称。您可以通过单击 SVM 名称查看有关目标 SVM 的更多详细信息。

- 目的地

  根据您的选择显示目标卷或 storage VM 的名称。您可以通过单击相应的对象名称来查看有关目标卷或 storage VM 的更多详细信息。

- 关系对象类型

  显示关系中使用的对象类型，例如 Storage VM、卷和一致性组。对于一致性关系中的对象，关系源和目标将显示一致性组，单击它们将转到 LUN 页面以查看关系。

- 策略

  显示 SnapMirror 关系的保护策略的名称。您可以单击策略名称以查看与该策略关联的详细信息，包括以下信息：

  - 传输优先级

    指定为异步操作运行传输的优先级。传输优先级为“正常”或“低”。“正常”优先级的传输会计划在“低”优先级的传输之前进行。默认值为“正常”。

  - 忽略访问时间

    仅适用于 SnapVault 关系。此选项用于指定增量传输是否忽略只更改了访问时间的文件。其值为“True”或“False”。默认值为“False”。

  - 当关系不同步时

    指定无法同步同步关系时 ONTAP 执行的操作。如果无法与辅助卷同步，StrictSync 关系将限制对主卷的访问。如果无法与辅助卷同步，Sync 关系不会限制对主卷的访问。

  - 尝试次数限制

    指定每次为 SnapMirror 关系执行手动传输或计划传输的最大尝试次数。默认值为 8。

  - 注释

    提供一个文本字段，用于为选定策略输入特定注释。

  - SnapMirror 标签

    指定与 Snapshot 副本策略关联的第一个计划的 SnapMirror 标签。如果要将 Snapshot 副本备份到 SnapVault 目标，则 SnapVault 子系统将使用此 SnapMirror 标签。

  - 保留设置

根据备份时间或备份数量指定备份的保留时间。

- 实际 Snapshot 副本

  指定此卷上与指定标签匹配的 Snapshot 副本的数量。

- 保留 Snapshot 副本

  指定即使达到策略最大限制也不会自动删除的 SnapVault Snapshot 副本的数量。其值为“True”或“False”。默认值为“False”。

- 保留警告阈值

  指定一个 Snapshot 副本限制，如果到达此限制，系统将发送警告，指出即将达到最大保留限制。

- 滞后持续时间

  显示镜像中的数据滞后于源的时间长度。

  对于 StrictSync 关系，延迟持续时间应接近或等于 0 秒。

- 滞后状态

  显示受管关系以及具有与该关系关联的计划的非受管关系的滞后状态。滞后状态可以是：

  - 错误

    滞后持续时间大于或等于滞后错误阈值。

  - 警告

    滞后持续时间大于或等于滞后警告阈值。

  - 确定

    滞后持续时间处于正常限制范围内。

  - 不适用

    滞后状态不适用于同步关系，因为无法配置计划。

- 上次成功更新

  显示上次成功执行 SnapMirror 或 SnapVault 操作的时间。

  上次成功更新不适用于同步关系。

- 成分关系

  显示所选对象中是否存在任何卷。

- 关系类型

显示用于复制卷的关系类型。关系类型包括：

- 异步镜像
- 异步存储
- 异步 MirrorVault
- StrictSync
- 同步

- 传输状态

显示保护关系的传输状态。传输状态可以是下列状态之一：

- 正在中止

  SnapMirror 传输已启用；但是，正在执行一个传输中止操作，此操作可能需要删除检查点。

- 正在检查

  正在对目标卷进行诊断检查，当前未进行传输。

- 正在完成

  SnapMirror 传输已启用。卷当前处于增量 SnapVault 传输的传输后阶段。

- 闲置

  已启用传输，但当前未进行传输。

- 同步

  处于同步关系的两个卷中的数据处于同步状态。

- 不同步

  目标卷中的数据与源卷不同步。

- 正在准备

  SnapMirror 传输已启用。卷当前处于增量 SnapVault 传输的传输前阶段。

- 已排队

  SnapMirror 传输已启用。当前未进行传输。

- 已暂停

  SnapMirror 传输已禁用。当前未进行传输。

- 正在暂停

  正在进行 SnapMirror 传输。其他传输已禁用。

- 正在传输

  已启用 SnapMirror 传输，且传输正在进行中。

- 正在过渡

  从源卷到目标卷的异步数据传输完成，并且已开始过渡到同步操作。

- 正在等待

  SnapMirror 传输已启动，但某些关联任务正在等待排队。

- 上次传输持续时间

  显示上次数据传输完成所用的时间。

  传输持续时间不适用于 StrictSync 关系，因为传输应同时进行。

- 上次传输大小

  显示上次数据传输的大小（以字节为单位）。

  传输大小不适用于 StrictSync 关系。

- 调解器

  显示调解器状态。

  - 不适用

    如果集群不支持 SnapMirror 活动同步。

  - 未配置

    如果未配置，或者已配置但仅添加了目标集群且未在 Unified Manager 中添加源集群。

  - 调解器 IP 地址

    如果已配置，并且源集群和目标集群都已添加到 Unified Manager 中。

- **State**

  显示 SnapMirror 或 SnapVault 关系的状况。该状况可以是“未初始化”、“已执行 SnapMirror”或“已断开”。如果选择源卷，则关系状况不适用，也不会显示。

- 关系健康状况

  显示集群的关系运行状况。

- 不健康的原因

  关系运行状况不正常的原因。

- 传输优先级

  显示传输的运行优先级。传输优先级为“正常”或“低”。“正常”优先级的传输会计划在“低”优先级的传输之前进行。

  传输优先级不适用于同步关系，因为所有传输的优先级均视为相同。

- 计划

  显示分配给关系的保护计划的名称。

  计划不适用于同步关系。

- 版本灵活复制

  显示“是”、“是，使用备份选项”或“无”。

- 源集群

  显示 SnapMirror 关系中的源集群的 FQDN、短名称或 IP 地址。

- **Source Cluster FQDN**

  显示 SnapMirror 关系中的源集群的名称。

- 源节点

  显示卷 SnapMirror 关系的源节点名称链接的名称，并在对象是 Storage VM 或一致性组时显示 SnapMirror 关系节点计数链接。

在自定义视图中，单击节点名称链接时，可以查看和扩展对这些一致性组的卷属于 SnapMirror 活动同步关系的存储对象的保护。

当您单击节点计数链接时，它会将您带到具有与此关系关联的相应节点的节点页面。当节点计数为 0 时，由于没有与此关系关联的节点，因此不会显示任何值。

- 目标节点

  显示卷的 SnapMirror 关系的目标节点名称链接的名称，并在对象为 Storage VM 或一致性组时显示 SnapMirror 关系节点计数链接。

  当您单击节点计数链接时，它会将您带到具有与此关系关联的相应节点的节点页面。当节点计数为 0 时，由于没有与此关系关联的节点，因此不会显示任何值。

- 目标集群

  显示 SnapMirror 关系中的目标集群的名称。

- 目标集群 **FQDN**

  显示 SnapMirror 关系中的目标集群的 FQDN、短名称或 IP 地址。

- 受保护

显示不同的关系。在此列中，您可以查看集群和存储虚拟机顺序的卷和一致性组关系，包括：

- SnapMirror
- Storage VM 灾难恢复
- SnapMirror，Storage VM 灾难恢复
- 一致性组
- SnapMirror，一致性组。

相关信息

- 有关*关系：MetroCluster*视图的信息，请参见 "监控 MetroCluster 配置"。
- 有关 关系：过去 **1** 个月的传输状态 视图的信息，请参阅 "关系：过去 1 个月的传输状态视图"。
- 有关*关系：所有关系*视图的信息，请参见 "关系：过去 1 个月的传输速率视图"。

在 **Active IQ Unified Manager** 中显示最近 **1** 个月传输状态视图

“关系：过去 1 个月的传输状态”视图使您能够分析异步关系中卷和 Storage VM 在一段时间内的传输趋势。此页面还会显示传输成功还是失败。

使用页面顶端的控件，您可以执行搜索以查找特定对象，创建和应用筛选器以缩小显示数据的列表，在页面上添加/删除/重新排序列，以及将页面上的数据导出为 `.csv`、 `.pdf` 或 `.xlsx` 文件。自定义页面后，您可以将结果保存为自定义视图，然后计划定期生成此数据的报告并通过电子邮件发送。您可以使用 **Filter** 选项仅查看选定的存储系统，例如仅查看卷或仅查看 Storage VMs。相同的报告显示在 Storage 页面中，且仅针对选定的存储实体显示。例如，如果要查看卷关系，您可以从 **Storage** > **Storage VMs** > **Relationship: Last 1 Month Transfer Status** 菜单或 **Protection** > **Relationships** > **Relationship: Last 1 Month Transfer Status** 菜单访问 Storage VMs 的 Relationship: Last 1 Month Transfer Status 报告，并使用 **Filter** 仅查看卷的数据。

- 源卷

  显示源卷名称。

- 目标卷

  显示目标卷名称。

- 操作类型

  显示卷传输的类型。

- 操作结果

  显示卷传输是否成功。

- 传输开始时间

  显示卷传输开始时间。

- 传输结束时间

显示卷传输结束时间。

- 传输持续时间

  显示完成卷传输所用的时间（以小时为单位）。

- 传输大小

  显示已传输卷的大小（以 MB 为单位）。

- 源 **SVM**

  显示存储虚拟机（SVM）名称。

- 源集群

  显示源集群名称。

- 目标 **SVM**

  显示目标 SVM 名称。

- 目标集群

  显示目标集群名称。

相关信息

- 有关*关系：所有关系*视图的信息，请参见 "关系：所有关系视图"。
- 有关 关系：**MetroCluster** 视图的信息，请参见 "监控 MetroCluster 配置"。
- 有关*关系：所有关系*视图的信息，请参见 "关系：过去 1 个月的传输速率视图"。

在 **Active IQ Unified Manager** 中显示关系：过去 **1** 个月传输速率视图

“关系：过去 1 个月的传输速率”视图使您能够分析异步关系中的卷每天传输的数据量。此页面还提供有关每日传输以及完成卷和 Storage VM 传输操作所需时间的详细信息。

页面顶部的控件使您能够执行搜索以查找特定对象，创建和应用筛选器以缩小显示数据的列表，在页面上添加/删除/重新排序列，并将页面上的数据导出为 .csv、.pdf 或 .xlsx 文件。自定义页面后，您可以将结果保存为自定义视图，然后计划定期生成此数据的报告并通过电子邮件发送。例如，如果要查看卷关系，您可以访问 **Storage > Volumes > Relationship: Last 1 Month Transfer Rate** 菜单或访问 **Protection > Relationships > Relationships:Last 1 Month Transfer Rate** 菜单，并使用 **Filter** 仅查看卷的数据。

- 总传输大小

  显示卷传输的总大小（以 GB 为单位）。

- 日

  显示启动卷传输的日期。

- 结束时间

  显示卷传输结束时间和日期。

相关信息

- 有关 关系：**MetroCluster** 视图的信息，请参见 "监控 MetroCluster 配置"。
- 有关 关系：过去 **1** 个月的传输状态 视图的信息，请参阅 "关系：过去 1 个月的传输状态视图"。
- 有关*关系：所有关系*视图的信息，请参见 "关系：过去 1 个月的传输速率视图"

生成自定义报告

Unified Manager 报告

了解 Active IQ Unified Manager 报告

Active IQ Unified Manager（以前称为 OnCommand Unified Manager）提供查看、自定义、下载和计划 ONTAP 存储系统报告的功能。这些报告可以提供有关存储系统容量、运行状况、性能、安全性和保护关系的详细信息。

Active IQ Unified Manager 9.6 中引入的新 Unified Manager 报告和调度功能取代了 Unified Manager 9.5 版本中停用的先前报告引擎。

报告提供网络的不同视图，提供有关容量、运行状况、性能、安全性和保护数据的可操作情报。您可以通过显示、隐藏和重新排列各列、筛选数据、排序数据以及搜索结果来自定义视图。您可以保存自定义视图以供重复使用，将其下载为报告，并将其安排为通过电子邮件分发的定期报告。

您可以下载 Microsoft® Excel 格式的视图并进行自定义。您可以使用高级 Excel 功能，例如复杂排序、分层筛选器、数据透视表和图表。当对生成的 Excel 报告感到满意时，您可以上传 Excel 文件，以便在每次安排和共享报告时使用。

除了从用户界面生成报告外，您还可以使用以下其他方法从 Unified Manager 中提取健康、安全和性能数据：

- 使用开放式数据库连接 (ODBC) 和 ODBC 工具直接访问数据库中的集群信息
- 执行 Unified Manager REST API 以返回您有兴趣查看的信息

从此版本的 Active IQ Unified Manager 开始，对报告进行了以下增强：

- 系统会根据配置的计划发送报告电子邮件。即使您生成按需报告，您也会收到一封电子邮件。
- 报告的文件名和元数据包含生成报告的主机名。即使有人更改了文件名，借助此增强功能，您仍然可以识别生成报告的主机名。

用于生成报告的访问点

探索在 **Active IQ Unified Manager** 中访问报告功能的三种方式

您可以在 Unified Manager 中收集有关群集的信息，以便从 UI、MySQL 数据库查询和 REST API 创建报告。

这些部分介绍了通过 UI 进行的 Unified Manager 报告和调度。

您可以通过三种方式访问 Unified Manager 提供的报告功能：

- 直接从 UI 中的清单页面提取数据。
- 使用开放式数据库连接（ODBC）和 ODBC 工具访问所有可用对象。
- 执行 Unified Manager REST API 以返回要查看的信息。

这些部分介绍了通过 UI 进行的 Unified Manager 报告和调度。

访问 **Active IQ Unified Manager** 中用于自定义报告的数据库

Unified Manager 使用 MySQL 数据库来存储来自其正在监视的集群的数据。数据持久化到 MySQL 数据库中的各种架构中。

支持访问以下数据库的所有数据表：

数据库	问题描述
netapp_model	ONTAP 控制器上的对象数据。
netapp_model_view	有关 ONTAP 控制器上的对象的数据，适合供报告工具使用。
netapp_performance	集群特定的性能计数器。
ocum	Unified Manager 应用程序数据和信息，以支持 UI 筛选、排序和一些派生字段的计算。
ocum_report	清单配置数据和容量相关信息。
ocum_report_birt	适合供报告工具使用的清单配置和容量相关数据的视图。
opm	性能配置设置和阈值信息。
scalemonitor	有关 Unified Manager 应用程序运行状况和性能问题的数据。
vmware_model	托管在 NetApp 存储上的数据存储的 VMware 对象数据。
vmware_model_view	托管在 NetApp 存储上的数据存储的 VMware 对象数据视图，适合供报告工具使用。
vmware_performance	NetApp 存储上托管的数据存储的 VMware 性能计数器数据。

报告用户（具有“报告架构”角色的数据库用户）能够访问这些表中的数据。此用户可直接从 Unified Manager 数据库以只读方式访问报告和其他数据库视图。请注意，此用户没有权限访问任何包含用户数据或集群凭据信息的表。

使用 **Active IQ Unified Manager REST API** 进行报告

您可以使用 REST API 来帮助管理集群，方法是查看 Unified Manager 捕获的运行状况、容量、性能和安全信息。

REST API 通过 Swagger 网页公开。您可以访问 Swagger 网页以查看 Unified Manager REST API 文档，以及手动发出 API 调用。在 Unified Manager Web UI 的菜单栏中，单击 **Help** 按钮，然后选择 **API Documentation**。有关 Unified Manager REST API 的信息，请参见 "Active IQ Unified Manager REST API 入门"。

要访问 REST API，您必须具有操作员、存储管理员或应用程序管理员角色。

了解 **Active IQ Unified Manager** 中的报告

报告显示有关存储、网络、服务质量和保护关系的详细信息，帮助您在潜在问题发生之前识别和解决问题。

自定义视图时，您可以使用唯一的名称保存视图，以备将来使用。您可以根据该视图计划定期运行报告并与其他人共享。您也可以以 Excel 格式下载视图，以使用高级 Excel 功能对其进行自定义，然后将该文件上传回 Unified Manager。如果您使用该视图计划报告，它将使用您上传的 Excel 文件来创建您可以共享的可靠报告。

您可以从“报告计划”页面管理已计划的所有报告。

要管理报告，您必须具有应用程序管理员或存储管理员角色。

您可以将报告下载为逗号分隔值（CSV）、Excel 或 PDF 文件。

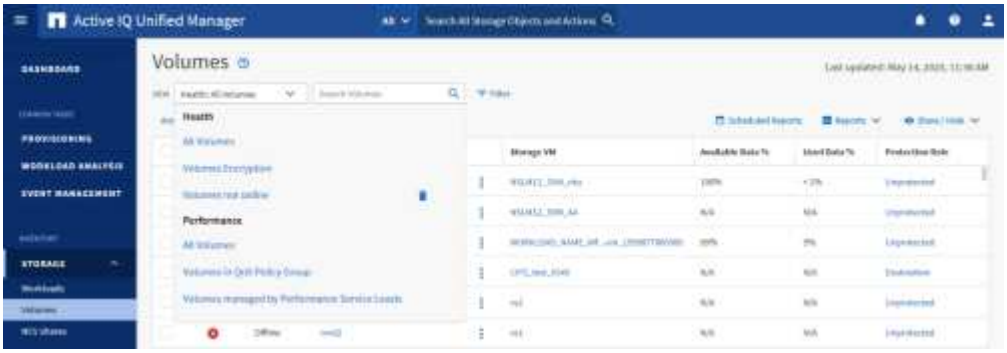
了解 **Active IQ Unified Manager** 中的视图和报告关系

下载或计划时，视图和清单页面将成为报告。

您可以自定义并保存视图和清单页面以供重复使用。您可以在 Unified Manager 中查看的几乎所有内容都可以保存、重复使用、自定义、计划并作为报告共享。

在视图下拉列表中，带有删除图标的项目是您或其他用户创建的现有自定义视图。没有图标的项目是 Unified Manager 提供的默认视图。默认视图无法修改或删除。

- 如果从列表中删除自定义视图，它还会删除使用该视图的所有 Excel 文件或计划报表。
- 如果您更改自定义视图，则使用该视图的报告将在下次根据报告计划生成并通过电子邮件发送报告时反映该更改。更改视图时，请确保您的更改适用于报告所使用的任何关联 Excel 自定义项。如果需要，您可以通过下载 Excel 文件、进行所需的更改，并将其作为该视图的新 Excel 自定义项上传来更新该文件。



只有具有应用程序管理员或存储管理员角色的用户才能看到删除图标，更改或删除视图，或者更改或删除计划报告。

了解 **Active IQ Unified Manager** 中的报告类型

此表提供了可作为报告提供的视图和清单页面的综合列表，您可以自定义、下载和计划这些视图和清单页面。

Active IQ Unified Manager 报告

类型	存储或网络对象
容量	集群 聚合 卷 qtree
运行状况	集群 节点 聚合 Storage VM 卷 SMB/CIFS 共享 NFS 共享
性能	集群 节点 聚合 Storage VM 卷 LUN 数 NVMe 命名空间 网络接口（LIF） 端口
服务质量 (QoS)	传统 QoS 策略组 自适应 QoS 策略组 性能服务级别策略组
卷保护关系（可从 Volumes 页面获取）	所有关系 过去 1 个月的传输状态 过去 1 个月的传输速率

类型	存储或网络对象
安全性	Storage VM 集群

了解 **Active IQ Unified Manager** 中的报告限制

请务必注意新的 Active IQ Unified Manager 报告功能存在一些限制。

来自早期版本的 **Unified Manager** 的现有报告

您只能编辑在 Unified Manager 9.5 及更早版本中创建并导入（作为 .rptdesign 文件）的现有报告的计划和收件人。如果您自定义了 Unified Manager 9.5 或更早版本提供的任何标准报告，则这些自定义报告不会导入到新的报告工具中。

如果需要编辑从 .rptdesign 文件导入的现有报告，请执行以下操作之一并删除导入的报告：

- 创建新视图并从该视图计划报告（首选）
- 将鼠标悬停在报告上，复制 SQL，并使用外部工具拉取数据

默认视图可以作为报告生成，而无需任何自定义。您可以使用新的报告解决方案重新创建任何自定义报告。

计划和报告关系

您可以为每个保存的报告创建多个不同的计划，其中包含任意收件人组合。但是，您不能对多个报告重复使用计划。

报告保护

任何具有相应权限的用户都可以编辑或删除报告。无法阻止其他用户删除或更改保存的视图或计划。

事件报告

虽然您可以自定义事件视图并以 CSV 格式下载生成的报告，但无法安排定期事件报告的生成和分发。

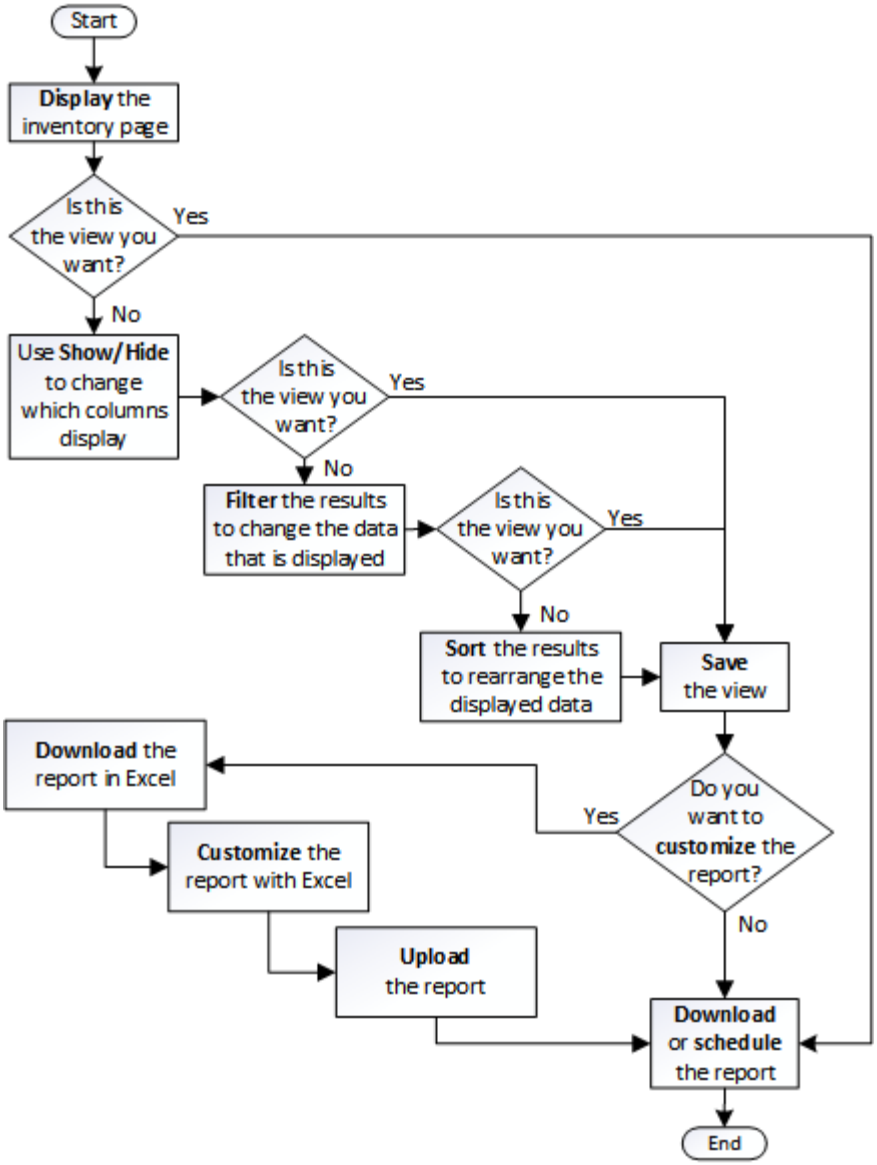
报告附件

报告不能在电子邮件正文中发送。相反，报告仅以 PDF、Excel 或 CSV 附件形式发送。

使用报告

了解 **Active IQ Unified Manager** 中的报告工作流

描述报告工作流的决策树。



开始使用 **Active IQ Unified Manager** 中的报告功能

创建自定义报表示例，以体验浏览视图和计划报表。此快速入门报表会查找可能要移动到云层的卷列表，因为存在相当数量的非活动（冷）数据。您将打开“性能：所有卷”视图，使用筛选器和列自定义视图，将自定义视图另存为报表，并安排报表每周共享一次。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须事先已配置 FabricPool 聚合，并且这些聚合包含一些卷。

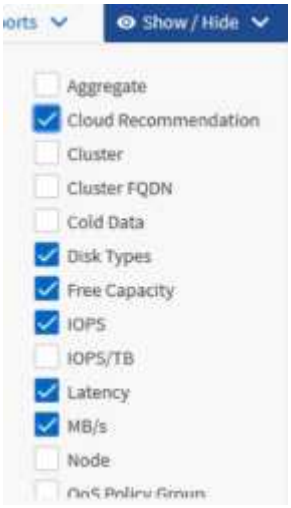
请按照以下步骤执行操作：

- 打开默认视图
- 通过筛选数据并对数据进行排序来自定义列
- 保存此视图

- 计划为此自定义视图生成报告

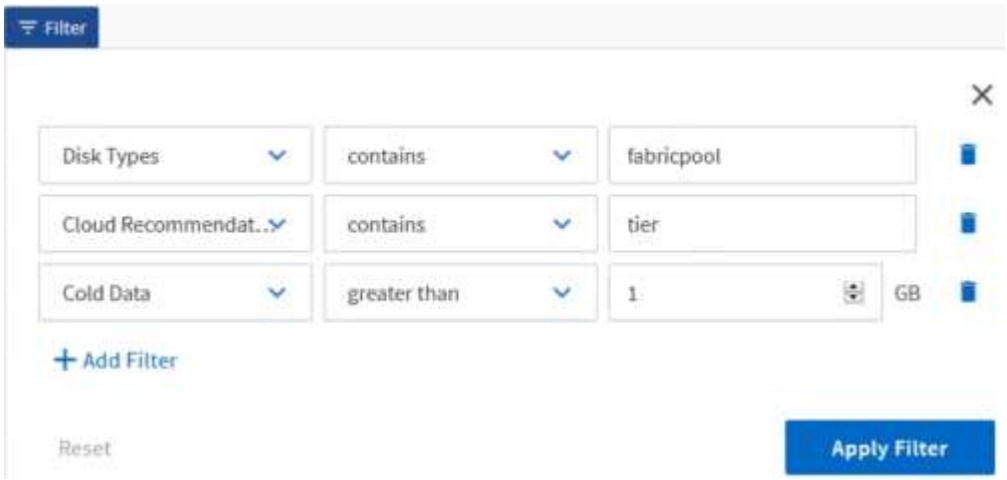
步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在“View”菜单中，选择 **Performance** > **All Volumes**。
3. 单击 显示/隐藏 以确保 “磁盘类型” 列显示在视图中。



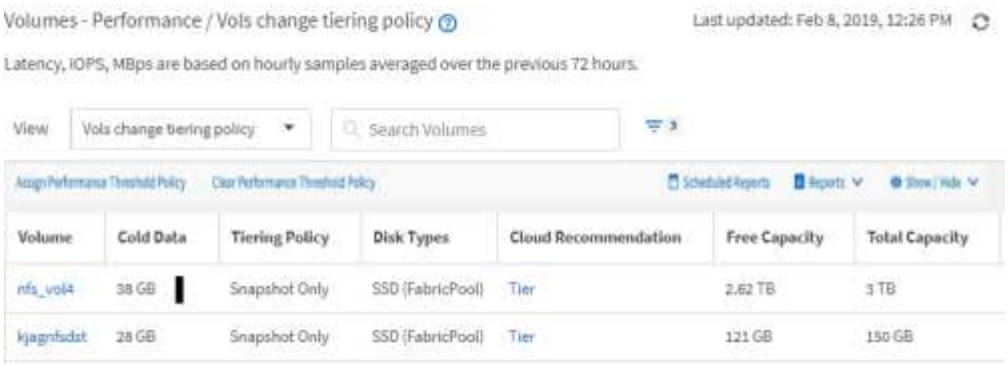
可添加或删除其他列以创建一个视图，其中包含对此报告重要的字段。

4. 将 “Disk Types” 列拖到 “Cloud Recommendation” 列旁边。
5. 单击筛选器图标以添加以下三个筛选器，然后单击*应用筛选器*：
   - 磁盘类型包含 FabricPool
   - “云建议”包含 tier
   - 冷数据大于 10 GB



请注意，每个筛选器都使用逻辑 AND 连接，因此返回的所有卷都必须满足所有条件。您最多可添加五个筛选器。

6. 单击冷数据列的顶部对结果进行排序，以便包含最多冷数据的卷显示在视图的顶部。
7. 自定义视图时，视图名称为“未保存的视图”。命名视图以反映视图显示的内容，例如“`Vols change tiering policy`”。完成后，单击复选标记或按 **Enter** 使用新名称保存视图。



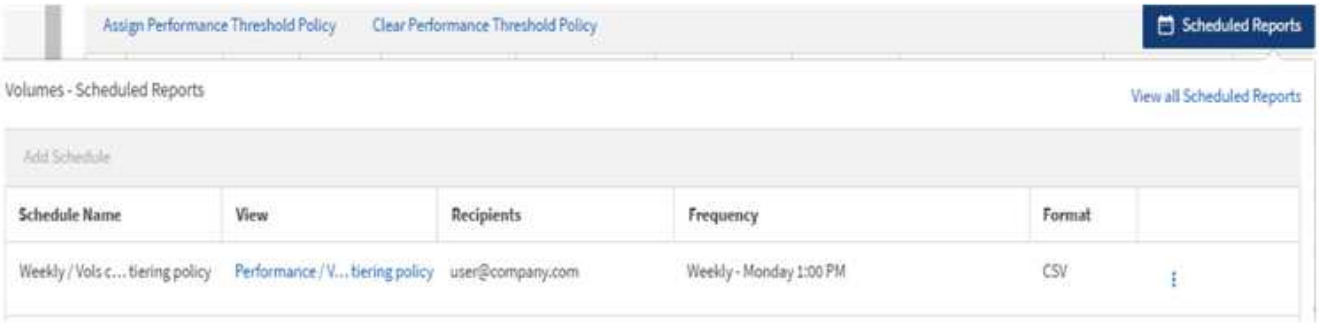
8. 将报告下载为 **CSV**、**Excel** 或 **PDF** 文件，以便在安排或共享之前查看输出。

   使用已安装的应用程序（如 Microsoft Excel（CSV 或 Excel）或 Adobe Acrobat（PDF））打开文件，或保存文件。

   > 您可以通过将视图下载为 Excel 文件，使用复杂的筛选器、排序、数据透视表或图表进一步自定义报告。在 Excel 中打开文件后，使用高级功能自定义报告。满意后，上传 Excel 文件。运行报告时，系统会将此文件及其自定义设置应用于视图。

   有关使用 Excel 自定义报告的详细信息，请参见 *Microsoft Excel* 报告示例。

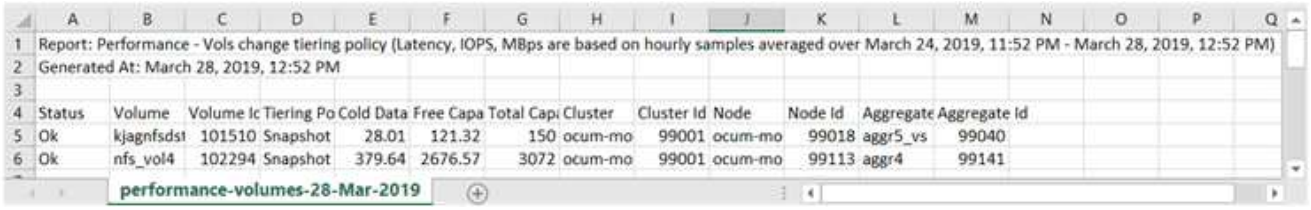
9. 单击清单页面上的*计划报告*按钮。与该对象（在本例中为卷）相关的所有计划报告都将显示在列表中。



10. 单击 **Add Schedule** 可在 Report Schedules 页面中添加新行，以便为新报告定义计划特征。
11. 输入报告的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

    以下示例报告采用 CSV 格式：



    以下示例报告采用 PDF 格式：



根据报告中显示的结果，您可能需要使用 ONTAP System Manager 或 ONTAP CLI 将某些卷的分层策略更改为“auto”或“all”，以便将更多冷数据卸载到云层。

在 **Active IQ Unified Manager** 中搜索计划报告

可以按名称、视图名称、对象类型或收件人搜索计划的报告。

1. 在左侧导航窗格中，单击*存储管理* > 报告计划。
2. 使用*搜索计划报告*文本字段。

要通过以下方式查找报告……	尝试……
计划名称	键入报告计划名称的一部分。
视图名称	键入部分报表视图名称。默认视图和自定义视图显示在视图列表中。
收件人	键入电子邮件地址的一部分。
文件类型	键入“PDF”、“CSV”或“XLSX”。

3. 您可以单击列标题，按该列升序或降序对报告进行排序，例如计划名称或格式。

自定义报告

在 **Active IQ Unified Manager** 中自定义报告

您可以通过多种方式自定义视图，以便创建包含管理 ONTAP 集群所需的所有信息的报告。

从默认清单页面或自定义视图开始，然后通过添加或删除列、更改列顺序、筛选数据或按升序或降序对特定列进行排序来对其进行自定义。

从 Unified Manager 9.8 开始，您还可以下载 Excel 格式的视图，以使用高级功能对其进行自定义。完成后，上传自定义的 Excel 文件。如果您使用该视图计划报告，它将使用自定义的 Excel 文件来创建您可以共享的强大报告。

有关使用 Excel 自定义报告的详细信息，请参见 *Microsoft Excel* 报告示例。

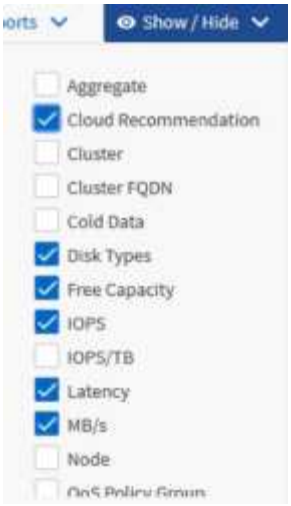
要管理报告，您必须具有应用程序管理员或存储管理员角色。

自定义 **Active IQ Unified Manager** 报告中的列

使用*显示/隐藏*选择要在报告中使用的列。拖动库存页面上的列以重新排列它们。

步骤

1. 单击*显示/隐藏*以添加或删除列。



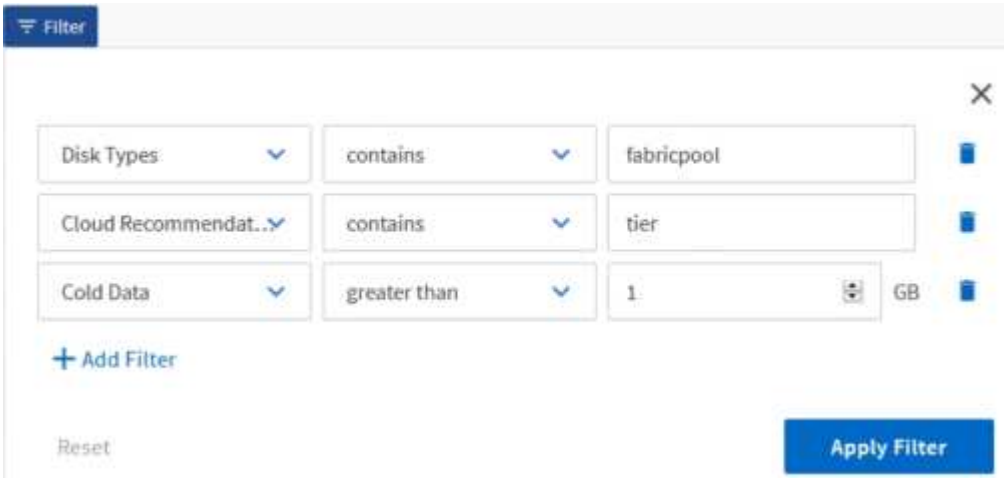
2. 在清单页面上，拖动列以按您在报告中所需的顺序对其进行重新排列。
3. 为未保存的视图命名以保存您的更改。

在 **Active IQ Unified Manager** 中筛选数据

筛选数据，以确保结果符合您的报告要求。筛选使您能够仅显示您感兴趣的数据。

步骤

1. 单击过滤器图标添加过滤器，以集中显示您要查看的结果，然后单击*应用过滤器*。



2. 为未保存的视图命名以保存您的更改。

在 **Active IQ Unified Manager** 中对数据排序

要对结果进行排序，请单击一列并指定升序或降序。对数据进行排序可优先显示报告所需的信息。

步骤

1. 单击列顶端对结果进行排序，使最重要的信息显示在视图顶端。
2. 为未保存的视图命名以保存您的更改。

搜索以优化您在 **Active IQ Unified Manager** 中的视图

在获得所需的视图后，您可以使用“搜索”字段进一步细化结果，以专注于要包含在报告中的结果。

步骤

1. 打开要用作报表基础的自定义或默认视图。
2. 在搜索字段中键入以细化视图中列出的数据。您可以在任何显示的列中输入部分数据。例如，如果要搜索名称中包含 "US_East" 的节点，则可以细化节点的完整列表。

   搜索结果将保存在自定义视图中，并在生成的计划报告中使用。

3. 为未保存的视图命名以保存您的更改。

使用 **Excel** 在 **Active IQ Unified Manager** 中自定义报告

保存视图后，您可以将其下载为 Excel 工作簿格式（.xlsx）。打开 Excel 文件时，您可以使用高级 Excel 功能自定义报告。

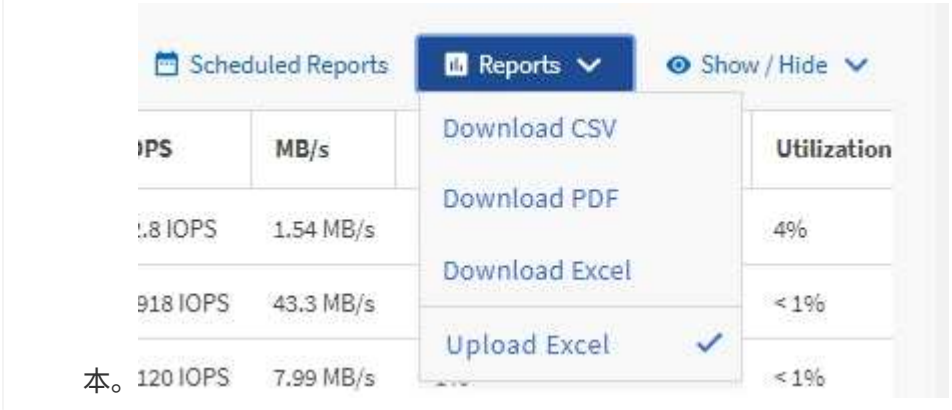
开始之前

您只能上传扩展名为 .xlsx 的 Excel 工作簿文件。

例如，您可以在报告中使用的一些高级 Excel 功能包括：

- 多列排序
- 复杂过滤
- 数据透视表
- 图表

- 下载的 Excel 文件使用视图的默认文件名，而不是保存的名称。
  - 格式为 `<View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx.`
  - 例如，名为 `Volumes-not online`的自定义保存视图如果在该日期和时间保存，其文件名为 `health-volumes-05-May-2020-19-18-00.xlsx`。
- 您可以向 Excel 文件添加工作表，但不能更改现有工作表。
  - 请勿更改现有工作表、数据和信息。相反，请将数据复制到您创建的新页面。
  - 上述规则的一个例外是，您可以在“data”页面上创建公式。使用数据页面公式在新页面上创建图表。
  - 请勿将新工作表命名为 data 或 info。
- 如果存在自定义 Excel 文件，则 报告 > 上传 **Excel** 菜单项旁边会有一个复选标记。当您下载 Excel 文件时，将使用带有自定义项的版



本。

步骤

1. 打开要用作报表基础的默认、自定义或已保存视图。
2. 选择 报告 > 下载 **Excel**。
3. 保存文件。文件已保存至您的下载文件夹。
4. 在 Excel 中打开保存的文件。请勿将该文件移动到新位置，或者如果您在其他位置进行工作，请在上传该文件之前使用原始文件名将该文件保存回原始位置。
5. 使用 Excel 功能（如复杂排序、分层筛选器、数据透视表或图表）自定义文件。有关详细信息，请参见 Microsoft® Excel 文档。
6. 选择 报告 > 上传 **Excel**，然后选择您修改的文件。最近下载的文件从相同的文件位置上传。
7. 使用*计划报告*功能向自己发送测试报告。

在 **Active IQ Unified Manager** 中下载报告

您可以下载报告并将数据以逗号分隔值（CSV）文件、Microsoft Excel（.XLSX）文件或 PDF 文件的形式保存到本地或网络驱动器。您可以使用电子表格应用程序（如 Microsoft Excel）打开 CSV 和 XLSX 文件，也可以使用阅读器（如 Adobe Acrobat）打开 PDF 文件。

步骤

1. 单击*报告*按钮将报告下载为以下格式之一：

选择	目的
下载 CSV	将报告保存为逗号分隔值 (CSV) 文件。
下载 PDF	将报告另存为 .pdf 文件。
下载 Excel	将报告另存为 Microsoft Excel (XLSX) 文件。

计划报告

在 **Active IQ Unified Manager** 中计划报告

拥有要重用并作为报告共享的视图后，您可以使用 Active IQ Unified Manager 对其进行计划。您可以管理计划报告，更改每个报告计划的收件人和分发频率。

您可以在 Unified Manager 中计划大多数视图或清单页面。例外情况是事件，这些报告您可以作为 CSV 文件下载，但不能计划重新生成和共享事件。您也不能下载或计划控制面板、收藏夹或配置页面。

从 Active IQ Unified Manager 9.8 开始，您可以下载 Microsoft® Excel 格式的视图并对其进行自定义。您可以使用高级 Excel 功能，例如复杂排序、分层筛选器、数据透视表和图表。如果对生成的 Excel 报表感到满意，您可以上传 Excel 文件，以便在每次安排和共享报表时使用。

您可以计划内置视图或您自定义的视图。您可以选择要发送的文件类型，可以是 CSV、PDF 或 XSLX。首次计划报告时，您可以下载该报告并将自己指定为唯一收件人，以便像您的收件人那样查看该报告。

计划报告

在 **Active IQ Unified Manager** 中计划报告

在您拥有要计划定期生成和分发的视图或 Excel 文件后，您可以计划该报表。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须在 常规 > 通知 页面中配置 SMTP 服务器设置，以便报告引擎可以将报告作为电子邮件附件从 Unified Manager 服务器发送到收件人列表。
- 必须将电子邮件服务器配置为允许使用生成的电子邮件发送附件。

使用以下步骤来测试和计划要为视图生成的报告。选择或自定义要使用的视图。以下过程使用显示网络接口性能的网络视图，但您可以使用任何所需的视图。

步骤

1. 打开视图。此示例使用显示 LIF 性能的默认网络视图。在左侧导航窗格中，单击 网络 **>** 网络接口。
2. 使用内置的 Unified Manager 功能根据需要自定义视图。
3. 自定义视图后，您可以在 视图 字段中提供一个唯一的名称，然后单击复选标记进行保存。



4. 您可以使用 Microsoft® Excel 的高级功能自定义报表。有关详细信息，请参见 "使用 Excel 自定义报告"。
5. 要在计划或共享输出之前查看输出，请执行以下操作：

选项	问题描述
如果使用 **Excel** 自定义报告	查看现有下载的 Excel 文件。
如果您没有使用 **Excel** 自定义报告	将报告下载为 **CSV**、**PDF** 或 **XLSX** 文件。

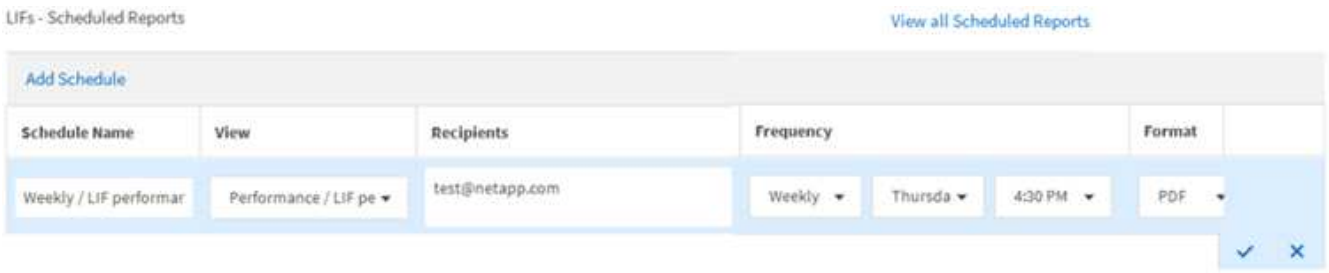
使用已安装的应用程序（例如 Microsoft Excel (CSV/XSLX) 或 Adobe Acrobat (PDF)）打开文件。

6. 如果对报告感到满意，请单击*计划报告*。
7. 在“报告计划”页面中，单击 添加计划。
8. 接受默认名称，这是视图名称和频率的组合，或自定义*计划名称*。

9. 要首次测试计划报告，请仅将您自己添加为*收件人*。满意后，添加所有报告收件人的电子邮件地址。
10. 指定生成报告并发送给收件人的频率。您可以选择*每日*、每周*或*每月。
11. 选择格式，可以是 **PDF**、**CSV** 或 **XSLX**。

    对于使用 Excel 自定义内容的报告，请始终选择 **XSLX**。

12. 单击复选标记（✓）以保存报告计划。



报告会立即作为测试发送。之后，报告将生成，并按计划的频率通过电子邮件发送给列出的收件人。

在 **Active IQ Unified Manager** 中计划导入的 **.rptdesign** 报告

您可以计划在早期版本的 Unified Manager 中创建和导入的现有报告。

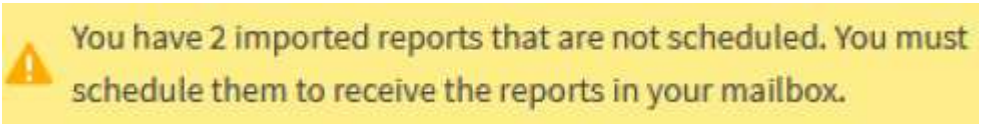
安排导入的报告需要满足以下条件：

- 在较早的 Unified Manager 版本中导入的 BIRT 设计的 .rptdesign 文件报告
- 升级到 Unified Manager 9.6 GA 或更高版本时适用

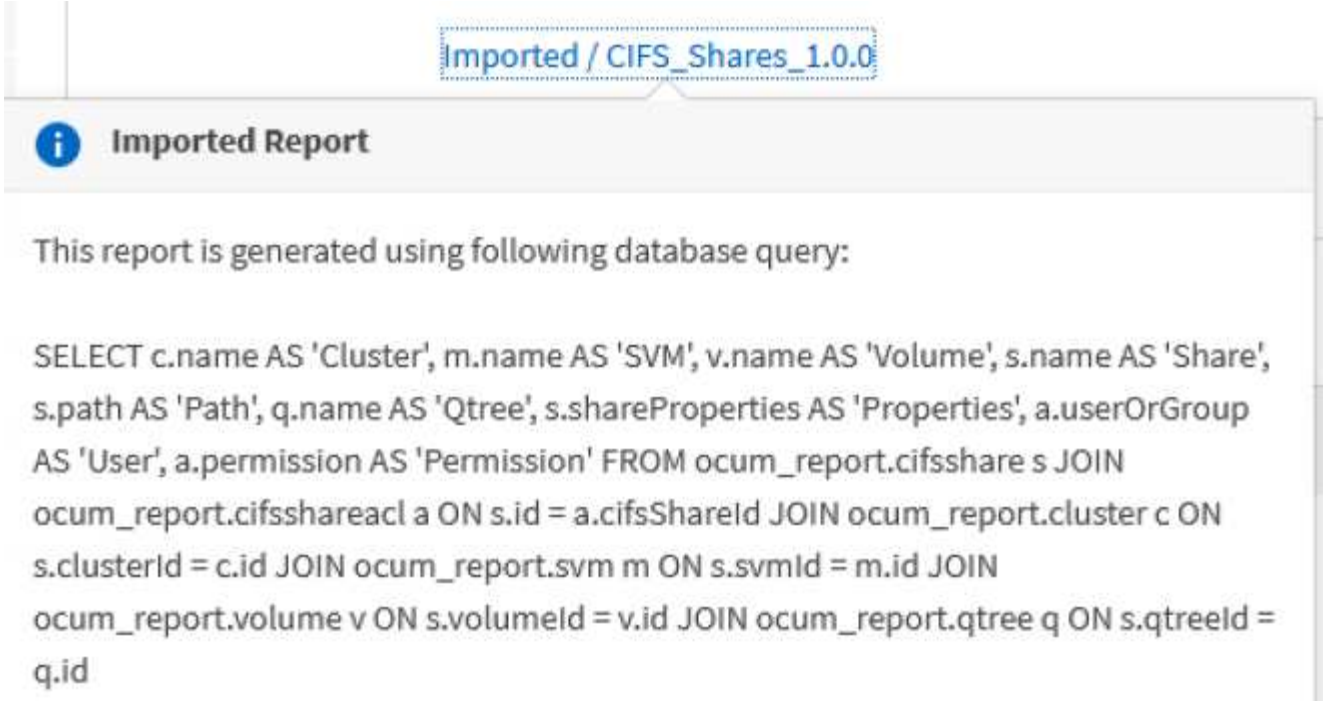
升级到 Unified Manager 9.6 GA 或更高版本后，报告计划页面将列出导入的报告。您可以编辑这些报告的计划，以指定收件人的电子邮件地址、频率和格式（PDF 或 CSV）。否则，无法在 Unified Manager UI 中编辑或查看这些报告。

步骤

1. 打开“报告计划”页面。如果您已导入报告，则会显示一条消息。



2. 单击*视图*名称以显示用于生成报告的 SQL 查询。



3. 单击更多图标 ⋮，单击*编辑*，定义报告计划详细信息，并保存此报告。

   您还可以通过“更多”图标 ⋮ 删除任何不需要的报告。

管理报告时间表

在 **Active IQ Unified Manager** 中管理报告计划

您可以从报告计划页面管理报告计划。您可以查看、修改或删除现有计划。

开始之前

您无法从“报告计划”页面安排新报告。您只能从对象清单页面添加计划报告。

- 您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 报告计划。
2. 在“报告计划”页面上：

目的	操作
查看现有计划	使用滚动条和页面控件滚动浏览现有报告列表。

目的	操作
编辑现有计划	a. 单击要使用的时间表的更多图标 ⋮。 b. 单击 **Edit**。 c. 进行必要的更改。 d. 单击复选标记以保存所做更改。
删除现有计划	a. 单击要使用的时间表的更多图标 ⋮。 b. 单击 **Delete**。 c. 请确认您的决定。

在 **Active IQ Unified Manager** 中编辑计划报告

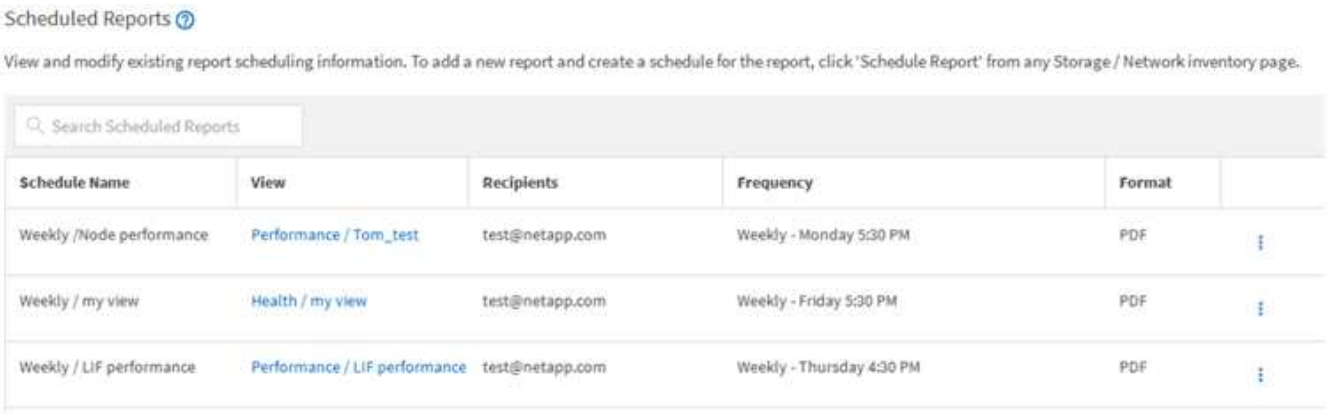
安排报告后，您可以在“报告计划”页面上对其进行编辑。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 报告计划。



ⓘ 如果您拥有适当的权限，则可以更改系统中的任何报告及其计划。

2. 单击要更改的时间表的更多图标 ⋮。
3. 单击 **Edit**。
4. 您可以更改报表计划的*计划名称*、收件人*列表、*频率*和*格式。
5. 完成后，单击复选标记以保存所做更改。

删除 **Active IQ Unified Manager** 中的计划报告

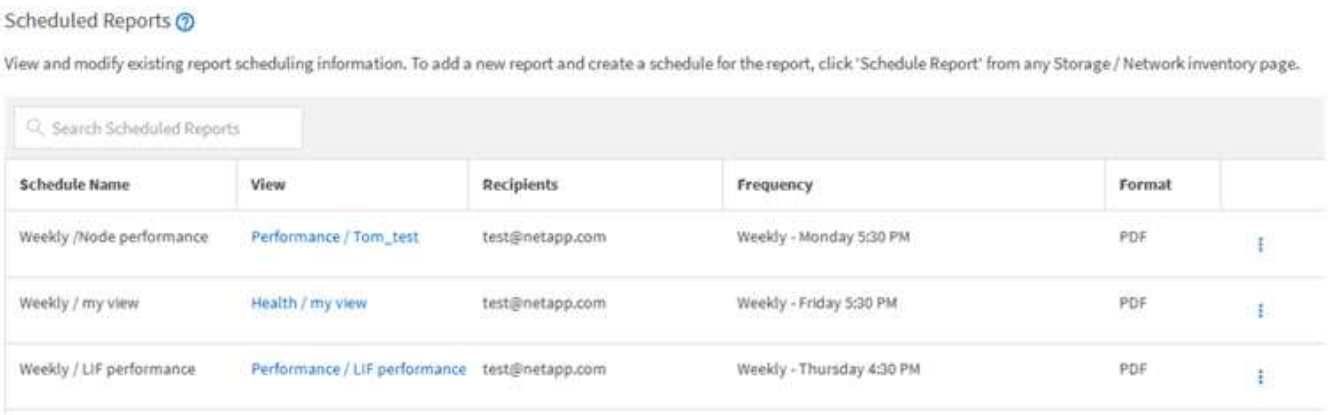
计划报告后，您可以从“报告计划”页面中将其删除。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 报告计划。



如果您拥有适当的权限，则可以删除系统中的任何报告及其计划。

2. 单击要删除的计划的“更多”图标 ⋮ 。
3. 单击 **Delete**。
4. 请确认您的决定。

   计划报告将从列表中删除，并且将不再按照设置的计划生成和分发。

如果从清单页面删除自定义视图，则使用该视图的任何自定义 Excel 文件或计划报表也将被删除。

自定义报告示例

了解 **Active IQ Unified Manager** 中的自定义报告示例

这些示例自定义报告通常用于帮助您识别潜在问题并在问题发生之前做出响应。

本节中的报告列表并非详尽无遗，并且会随着时间的推移而增加。您可以通过提供文档反馈，建议将自定义报告添加到本节中。

要管理报告，您必须具有应用程序管理员或存储管理员角色。

自定义集群存储报告

在 **Active IQ Unified Manager** 中创建报告以按集群型号查看容量

您可以创建报告，以基于存储系统模型分析集群的存储容量和利用率。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建按群集模型显示容量的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 存储 > 集群。
2. 在 View 菜单中，选择 **Capacity** > **All Clusters**。
3. 选择 显示/隐藏 以删除报告中您不希望出现的任何列，例如 “Cluster FQDN” 和 “OS Version”。
4. 将“总原始容量”、“型号 / 系列”和三个聚合列拖到“集群”列附近。
5. 单击 “Model/Family” 列的顶部，按集群类型对结果进行排序。
6. 使用反映视图显示内容的特定名称保存视图，例如“`Capacity by Cluster Model`”。
7. 单击清单页面上的 **Scheduled Reports** 按钮。
8. 单击*添加计划*可将新行添加到*报告计划*页面，以便您可以定义新报告的计划特性。
9. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要向某些群集添加更多容量，或升级较旧的群集型号。

在 **Active IQ Unified Manager** 中识别具有未分配 **LUN** 容量的集群

您可以创建报告以查找具有最多未分配 LUN 容量（大于 0.5 TB）的集群，以帮助确定可以在何处添加额外的工作负载。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建显示未分配 LUN 容量最大的集群的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 存储 > 集群。
2. 在 View 菜单中，选择 **Capacity** > **All Clusters**。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 将 “Unallocated LUN Capacity” 列拖至 “HA Pair” 列附近。
5. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - 未分配的 LUN 容量大于 0.5 TB
6. 单击 “未分配的 LUN 容量” 列的顶部，按最大未分配 LUN 容量对结果进行排序。
7. 使用反映视图显示内容的特定名称保存视图，例如“大多数未分配的 `LUN` 容量”，然后单击复选标记（✓）。
8. 单击清单页面上的 **Scheduled Reports** 按钮。
9. 单击*添加计划*可将新行添加到“报告计划”页面，以便您可以定义新报告的计划特性。

10. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要使用群集的未分配 LUN 容量。

创建报告以查看 **Active IQ Unified Manager** 中可用容量最多的 **HA** 对

您可以创建一个报告来查找容量最大的高可用性（HA）对，以调配新卷和 LUN。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建一个自定义视图，该视图显示按最可用容量排序的 HA 对，以配置新卷和 LUN，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 存储 > 集群。
2. 在 View 菜单中，选择 **Capacity** > **All Clusters**。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 将“`Aggregate Unused Capacity`”列拖到“`HA Pair`”列附近。
5. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
    - 聚合未用容量大于 0.5 TB
6. 单击 “Aggregate Unused Capacity” 列的顶部，按未使用的聚合容量最大值对结果进行排序。
7. 使用反映视图显示内容的特定名称保存视图，例如“最少使用的聚合容量”，然后单击复选标记（✓）。
8. 单击清单页面上的 **Scheduled Reports** 按钮。
9. 单击*添加计划*可将新行添加到“报告计划”页面，以便您可以定义新报告的计划特性。
10. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要根据聚合容量平衡 HA 对。

创建报告以查看在 **Active IQ Unified Manager** 中运行旧版 **ONTAP** 的节点

您可以创建报告以显示所有集群节点上安装的 ONTAP 软件的版本，以便查看要升级的节点。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建一个自定义视图，以显示运行旧版本 ONTAP 的节点，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击*存储* > 节点。

2. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
3. 将 “OS Version” 列拖到 “Node” 列附近。
4. 单击“`OS Version`”列的顶部，以按最旧的 ONTAP 版本对结果进行排序。
5. 使用反映视图显示内容的特定名称保存视图，例如“`Nodes by ONTAP 版本`”。
6. 单击清单页面上的 **Scheduled Reports** 按钮。
7. 单击*添加计划*可将新行添加到“报告计划”页面，以便您可以定义新报告的计划特性。
8. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要升级运行较旧 ONTAP 版本的节点。

自定义聚合容量报告

创建报告以查看 **Active IQ Unified Manager** 中容量接近上限的聚合

您可以创建报告以查找接近满容量的聚合，以便添加更多容量或将工作负载移动到其他聚合。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤来创建显示达到满容量的聚合的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击*存储* > 聚合。
2. 在“View”菜单中，选择 **Capacity** > **All Aggregates**。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - 达到满载的天数少于 45 天
5. 单击 “Days to Full” 列顶部，按达到满容量的剩余天数从少到多对结果进行排序。
6. 使用反映视图显示内容的特定名称保存视图，例如 “Days to full aggregate capacity”，然后单击复选标记（✓）。
7. 单击清单页面上的 **Scheduled Reports** 按钮。
8. 单击*添加计划*可将新行添加到*报告计划*页面，以便您可以定义新报告的计划特性。
9. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要为达到满容量的聚合增加存储空间。此外，您可能希望将“距离满容量的天数”阈值增加到超过默认的 7 天，以便在收到事件后有更多时间来应对聚合空间不足的情况。

创建报告以查看 **Active IQ Unified Manager** 中已满 **80%** 或更多的聚合

您可以创建报告以突出显示已满 80% 或以上的聚合。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建一个自定义视图，以显示已满 80% 或以上的聚合，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击*存储* > 聚合。
2. 在“View”菜单中，选择 **Capacity** > **All Aggregates**。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 将 "\`可用数据 %\`" 和 "\`已用数据 %\`" 列拖到 "\`聚合\`" 列附近。
5. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - 已用数据 % 大于 80%
6. 单击 “已用数据 %” 列的顶部，按容量百分比对结果进行排序。
7. 使用反映视图显示内容的特定名称保存视图，例如“聚合接近满”，然后单击复选标记（✓）。
8. 单击清单页面上的 **Scheduled Reports** 按钮。
9. 单击*添加计划*可将新行添加到“报告计划”页面，以便您可以定义新报告的计划特性。
10. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要从某些聚合中移动一些数据。

创建报告以查看在 **Active IQ Unified Manager** 中过量使用的聚合

您可以创建报告以分析存储容量和聚合使用情况，并查看过度提交的聚合。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建自定义视图，以显示超出超额配置阈值的聚合，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击*存储* > 聚合。
2. 在“View”菜单中，选择 **Capacity** > **All Aggregates**。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 将“`Overcommitted Capacity %`”列拖到“`Aggregate`”列附近。
5. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - 过量提交的容量 % 大于 100%

6. 单击 “过度配置容量 %” 列的顶部，按容量百分比对结果进行排序。
7. 使用反映视图显示内容的特定名称保存视图，例如“`Aggregates overcommitted`”，然后单击复选标记（✓）。
8. 单击清单页面上的 **Scheduled Reports** 按钮。
9. 单击*添加计划*可将新行添加到“报告计划”页面，以便您可以定义新报告的计划特性。
10. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要为聚合添加更多容量，或从某些聚合中移动一些数据。

自定义卷容量报告

在 **Active IQ Unified Manager** 中识别已禁用 **Snapshot** 自动删除且接近容量上限的卷

您可以创建一个报告，其中包含已禁用 Snapshot 自动删除功能且接近满容量的卷列表。这些结果有助于确定可能需要配置 Snapshot 自动删除的卷。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

按照以下步骤创建以正确顺序显示所需列的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在 View 菜单中，选择 **Capacity** > **All Volumes**。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 将 “Snapshot 自动删除” 和 “Days To Full” 列拖放到 “Available Data Capacity” 列附近。
5. 单击过滤器图标，添加以下两个过滤器，然后单击*应用过滤器*：
   - 距离全满天数少于 30 天
   - Snapshot 自动删除已禁用
6. 单击 距离全满天数 列顶端，以便剩余天数最少的卷显示在列表顶端。
7. 使用反映视图显示内容的特定名称保存视图，例如 “Vols near capacity”。
8. 单击清单页面上的 **Scheduled Reports** 按钮。
9. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要在卷上启用 Snapshot 自动删除，或者想办法增加可用空间。

识别 **Active IQ Unified Manager** 中已禁用精简配置的卷

当卷未精简配置时，它会占用创建卷时定义的磁盘上的全部空间量。识别已禁用精简配置

的卷有助于确定是否要在某些卷上启用精简配置。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

按照以下步骤创建以正确顺序显示所需列的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在 View 菜单中，选择 **Capacity** > **All Volumes**。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 将 “已用数据 %” 和 “已精简配置” 列拖放到 “可用数据容量” 列附近。
5. 单击筛选器图标，添加以下筛选器，精简配置*为*否，然后单击*应用筛选器*。
6. 单击 "\`已用数据 %\`" 列顶端对结果进行排序，使百分比最高的卷显示在列表顶端。
7. 使用能够反映视图显示内容的名称保存视图，例如“`Vols no thin provisioning`”。
8. 单击清单页面上的 **Scheduled Reports** 按钮。
9. 单击*添加计划*以将新行添加到*报告计划*页面，以便您可以定义新报告的计划特性。
10. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✔）。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要在某些卷上启用精简配置。

确定应在 **Active IQ Unified Manager** 中将数据移至云层的卷

您可以创建一个报告，其中包含当前驻留在 FabricPool 聚合上、云建议为 Tier 且具有大量冷数据的卷列表。此报告可帮助您决定是否应将某些卷的分层策略更改为 “auto” 或 “all”，以将更多冷（非活动）数据卸载到云层。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须事先已配置 FabricPool 聚合，并且这些聚合包含一些卷。

按照以下步骤创建以正确顺序显示所需列的自定义视图，然后计划为该视图生成报告。

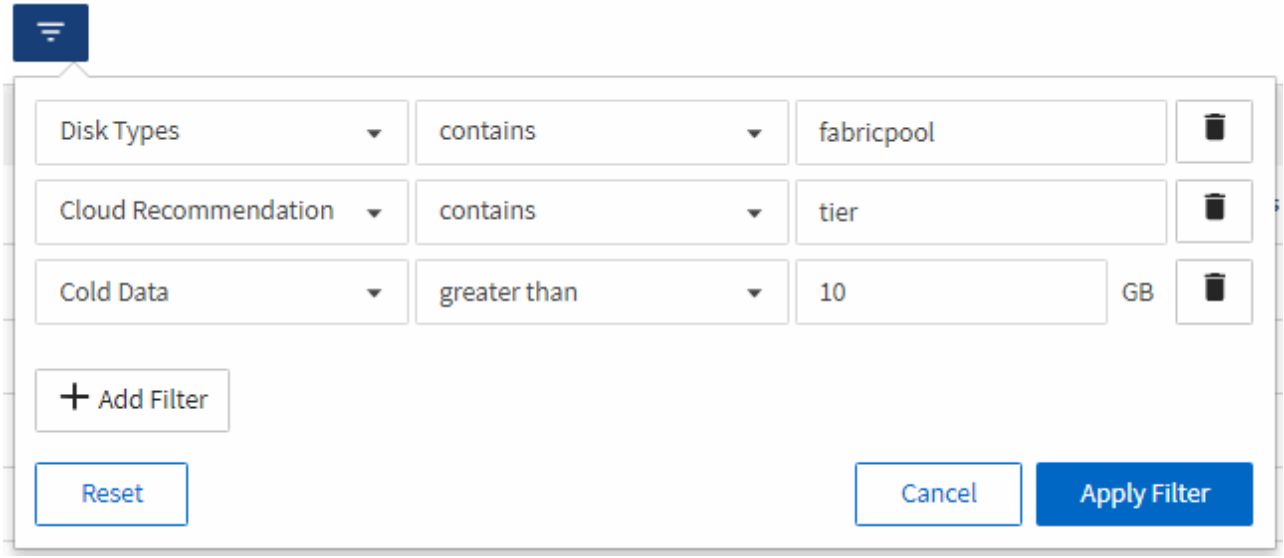
步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在“View”菜单中，选择 **Performance** > **All Volumes**。
3. 在列选择器中，确保在视图中显示 “磁盘类型” 列。

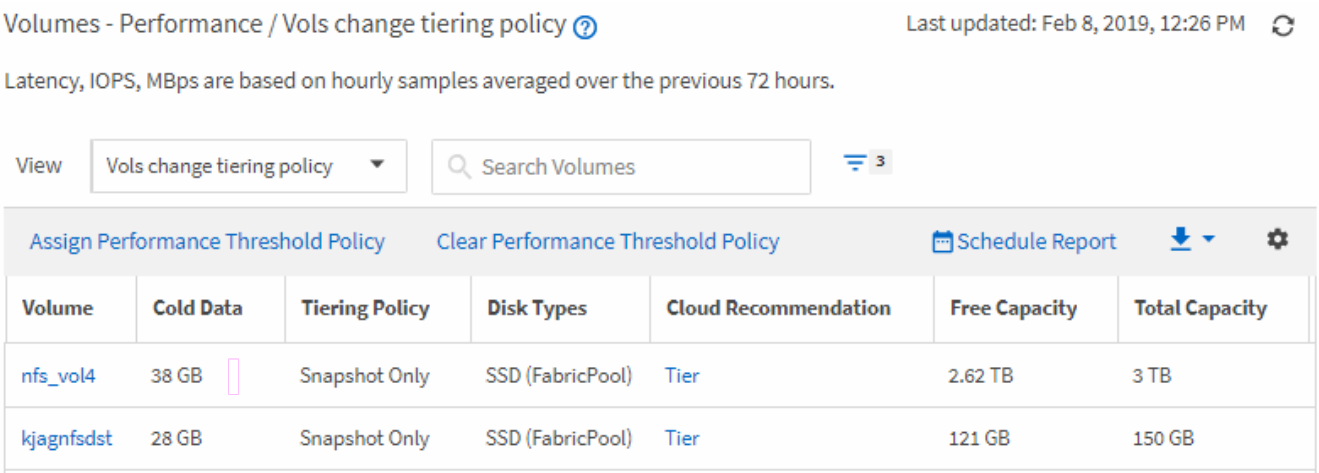
   添加或删除其他列以创建对您的报告很重要的视图。

4. 将 “Disk Type” 列拖放到 “Cloud Recommendation” 列附近。

5. 单击过滤器图标，添加以下三个过滤器，然后单击*应用过滤器*：
   - 磁盘类型包含 FabricPool
   - “云建议”包含 tier
   - 冷数据大于 10 GB



6. 单击冷数据列的顶部，使包含最多冷数据的卷显示在视图的顶部。
7. 使用反映视图显示内容的名称保存视图，例如 “Vols change tiering policy”
。



8. 单击清单页面上的 **Scheduled Reports** 按钮。
9. 单击*添加计划*可将新行添加到“报告计划”页面，以便您可以定义新报告的计划特性。
10. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要使用 System Manager 或 ONTAP CLI 将某些卷的分层策略更改为 “auto” 或 “all”，以便将更多冷数据卸载到云层。

自定义 **Qtree** 容量报告

创建报告以查看 **Active IQ Unified Manager** 中几乎已满的 **qtree**

您可以创建报告来分析 qtree 的存储容量和利用率，并查看几乎已满的 qtree。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建显示接近满的 qtree 的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 存储 > **Qtrees**。
2. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
3. 将 “Disk Used %” 列拖到 “Qtrees” 列附近。
4. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - 磁盘已用 % 大于 75%
5. 单击 “Disk Used %” 列的顶部，按容量百分比对结果进行排序。
6. 使用反映视图显示内容的特定名称保存视图，例如“`Qtrees nearing full`”，然后单击复选标记（✓）。
7. 单击清单页面上的 **Scheduled Reports** 按钮。
8. 单击*添加计划*以将新行添加到*报告计划*页面，以便您可以定义新报告的计划特性。
9. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要调整磁盘硬限制和软限制（如果已设置），或在 qtree 之间平衡数据。

自定义 **NFS** 共享报告

在 **Active IQ Unified Manager** 中自定义 **NFS** 共享报告

您可以自定义 NFS 共享报告，以分析有关存储系统上卷的 NFS 导出策略和规则的信息。例如，您可以自定义报告以显示装载路径不可访问的卷以及具有默认导出策略的卷。

创建报告以查看 **Active IQ Unified Manager** 中挂载路径不可访问的卷

您可以创建报告以查找装载路径不可访问的卷。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤为装载路径不可访问的卷创建自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击*存储* > **NFS** 共享。
2. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
3. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - 挂载路径活动为否
4. 使用反映视图显示内容的特定名称保存视图，例如“具有无法访问的装载路径的卷”，然后单击复选标记（✓）。
5. 单击清单页面上的 **Scheduled Reports** 按钮。
6. 单击 **Add Schedule** 可在 Report Schedules 页面中添加新行，以便为新报告定义计划特征。
7. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要更正无法访问的挂载路径。

创建报告以查看在 **Active IQ Unified Manager** 中使用默认导出策略的卷

您可以创建报告以查找正在使用默认导出策略的卷。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤为使用默认导出策略的卷创建自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击*存储* > **NFS** 共享。
2. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
3. 将 “导出策略” 列拖到 “卷” 列附近。
4. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - 导出策略包含默认值
5. 使用反映视图显示内容的特定名称保存视图，例如“使用默认导出策略的卷”，然后单击复选标记（✓）。
6. 单击清单页面上的 **Scheduled Reports** 按钮。
7. 单击 **Add Schedule** 可在 Report Schedules 页面中添加新行，以便为新报告定义计划特征。
8. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要配置自定义导出策略。

自定义 **storage VM** 报告

在 **Active IQ Unified Manager** 中自定义存储 **VM** 报告

您可以创建存储 VM 报告来分析卷信息并查看整体运行状况和存储可用性。例如，您可以

创建报告来显示达到最大卷计数的 SVM 并分析已停止的 SVM。

创建报告以查看在 **Active IQ Unified Manager** 中达到最大卷限制的存储 **VM**

您可以创建报告以查找达到最大卷限制的 SVM。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建显示达到最大卷限制的存储 VM 的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 存储 > 存储 **VM**。
2. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
3. 将“Volume Count”和“Maximum Allowed Volumes”列拖到“Storage VM”列附近。
4. 单击 “Maximum Allowed Volumes” 列的顶部，按最高卷数对结果进行排序。
5. 使用反映视图显示内容的特定名称保存视图，例如“SVM 达到最大卷”，然后单击复选标记（✓）。
6. 单击清单页面上的 **Scheduled Reports** 按钮。
7. 单击*添加计划*可将新行添加到*报告计划*页面，以便您可以定义新报告的计划特性。
8. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要平衡分配给存储 VM 的卷，或者在可能的情况下，使用 ONTAP System Manager 更改允许的最大卷数。

创建报告以查看 **Active IQ Unified Manager** 中已停止的存储 **VM**

您可以创建报告以显示所有停止的 SVM 的列表。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建显示已停止的存储 VM 的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 存储 > 存储 **VM**。
2. 在 View 菜单中，选择 **Health** > **All Storage VMs**。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 将"`State`"列拖到"`Storage VM`"列附近。
5. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - 状态为已停止
6. 使用反映视图显示内容的特定名称保存视图，例如“已停止的 SVM”，然后单击复选标记（✓）。

7. 单击清单页面上的 **Scheduled Reports** 按钮。
8. 单击*添加计划*可将新行添加到*报告计划*页面，以便您可以定义新报告的计划特性。
9. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要调查 SVM 停止的原因，以确定是否应重新启动已停止的 SVM。

自定义卷关系报告

在 **Active IQ Unified Manager** 中自定义卷关系报告

“卷关系清单”报告使您可以分析集群中的存储清单详细信息，了解卷所需的保护级别，并根据故障源、模式和计划来筛选卷详细信息。

在 **Active IQ Unified Manager** 中创建报告，按故障来源对卷关系进行分组

您可以创建一个报告，按关系处于不正常状态的原因对卷进行分组。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建按故障源对卷进行分组的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在“视图”菜单中，选择 关系 > 所有关系。
3. 选择 显示/隐藏 以确保 “关系健康” 和 “不健康原因” 列显示在视图中。

   添加或删除其他列以创建对您的报告很重要的视图。

4. 将 “Relationship Health” 和 “Unhealthy Reason” 列拖到 “State” 列附近。
5. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - 关系运行状况不佳
6. 单击 “Unhealthy Reason” 列的顶部，按故障源对卷关系进行分组。
7. 使用反映视图显示内容的特定名称保存视图，例如“`Vol relationships by failure`”。
8. 单击清单页面上的 **Scheduled Reports** 按钮。
9. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可以调查每种类型故障的来源和影响。

在 **Active IQ Unified Manager** 中创建报告以按问题对卷关系进行分组

您可以创建一个按问题对卷关系进行分组的报告。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建一个自定义视图，按问题对卷关系进行分组，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在“视图”菜单中，选择 关系 > 所有关系。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 将 “Unhealthy Reason” 列拖到 “State” 列附近。
5. 单击 “不健康原因” 列的顶部，按问题对卷进行分组。
6. 使用反映视图显示内容的特定名称保存视图，例如“`Vol relationships by issue`”。
7. 单击清单页面上的 **Scheduled Reports** 按钮。
8. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✔）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

您可以根据报告中显示的结果，调查每种类型问题的来源和影响。

创建报告以在 **Active IQ Unified Manager** 中按时间间隔查看卷传输趋势

您可以创建一个报告，以特定时间间隔显示卷传输趋势。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤以特定时间间隔创建卷的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在视图菜单中，选择*关系* > 过去 **1** 个月的传输状态。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 将传输持续时间列拖到“操作结果”列附近。
5. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - 过去 7 天内的传输结束时间
6. 单击 “传输持续时间” 列的顶部，按时间间隔对卷进行排序。
7. 使用反映视图显示内容的特定名称保存视图，例如“按持续时间排列的卷”。
8. 单击清单页面上的 **Scheduled Reports** 按钮。

9. 输入报告计划的名称，将频率设置为*每周*，并填写其他报告字段，然后单击行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可以调查传输时间间隔。

创建报表以查看 **Active IQ Unified Manager** 中失败或成功的卷传输

您可以创建显示卷传输状态的报告。您可以在此报告中查看失败和成功的卷传输。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建自定义视图，以显示哪些传输失败，哪些传输成功，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在视图菜单中，选择*关系* > 过去 **1** 个月的传输状态。
3. 选择*显示/隐藏*以删除报告中不希望出现的任何列。
4. 将 “Operation Result” 列拖到 “State” 列附近。
5. 单击 “操作结果” 列的顶部，按状态对卷进行排序。
6. 使用反映视图显示内容的特定名称保存视图，例如“`Volumes by transfer status`”。
7. 单击清单页面上的 **Scheduled Reports** 按钮。
8. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可以调查传输状态。

在 **Active IQ Unified Manager** 中创建报告以按传输大小查看卷传输

您可以创建报告，以根据传输大小查看卷传输。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建基于传输大小的卷传输的自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在查看菜单中，选择 关系 > 过去 **1** 个月的传输速率。
3. 单击 “Total Transfer Size” 列的顶部，按大小对卷传输进行排序。
4. 使用反映视图显示内容的特定名称保存视图，例如“`Volumes by transfer size`”。
5. 单击清单页面上的 **Scheduled Reports** 按钮。

6. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可以按传输大小调查卷关系。

创建报告以查看 **Active IQ Unified Manager** 中按天分组的卷传输

您可以创建报告以查看按天分组的卷传输。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤为按天分组的卷传输创建自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在查看菜单中，选择 关系 > 过去 **1** 个月的传输速率。
3. 单击“Day”列的顶部，按天对卷传输进行排序。
4. 使用反映视图显示内容的特定名称保存视图，例如“按天进行卷传输”。
5. 单击清单页面上的 **Scheduled Reports** 按钮。
6. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可以按天调查卷传输。

自定义卷性能报告

在 **Active IQ Unified Manager** 中创建报告以识别非 **FabricPool** 聚合上具有高冷数据的卷

您可以创建报告，以显示非 FabricPool 聚合上具有大量冷数据的卷。这可以帮助您识别应移动到 FabricPool 聚合的卷。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤为在未启用 FabricPool 的聚合上具有大量冷数据的卷创建自定义视图，然后计划为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在“View”菜单中，选择 **Performance** > **All Volumes**。
3. 选择*显示/隐藏*以确保 "\`磁盘类型\`" 列显示在视图中。

   添加或删除其他列以创建对您的报告很重要的视图。

4. 将 “磁盘类型” 列拖到 “冷数据” 列附近。
5. 单击过滤器图标，添加以下过滤器，然后单击*应用过滤器*：
   - “冷数据”大于 100 GB
   - 磁盘类型包含 SSD
6. 单击“**磁盘类型**”列的顶端，按磁盘类型对卷进行排序，以便磁盘类型 SSD （FabricPool） 位于底端。
7. 使用反映视图显示内容的特定名称保存视图，例如“`Cold data vols not FabricPool`”。
8. 单击清单页面上的 **Scheduled Reports** 按钮。
9. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

   此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可以找到适合移动到 FabricPool 聚合的候选卷。

Microsoft Excel 报告示例

了解 Active IQ Unified Manager 中的 Microsoft Excel 示例报告

这些 Microsoft Excel 示例报告旨在介绍使用 Excel 高级功能提供的报告选项。

Excel 的高级功能可以创建各种特定于您需求的报告。有关如何使用 Excel 的完整信息，请参见产品文档。

要管理报告，您必须具有应用程序管理员或存储管理员角色。

创建报告以在 Active IQ Unified Manager 中显示聚合容量表和图表

您可以使用总计和簇状柱形图格式创建报表，以分析 Excel 文件中的容量。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤打开运行状况：所有聚合视图，在 Excel 中下载视图，创建可用容量图表，上传自定义的 Excel 文件，并计划最终报告。

步骤

1. 在左侧导航窗格中，单击*存储* > 聚合。
2. 选择 报告 > 下载 **Excel**。



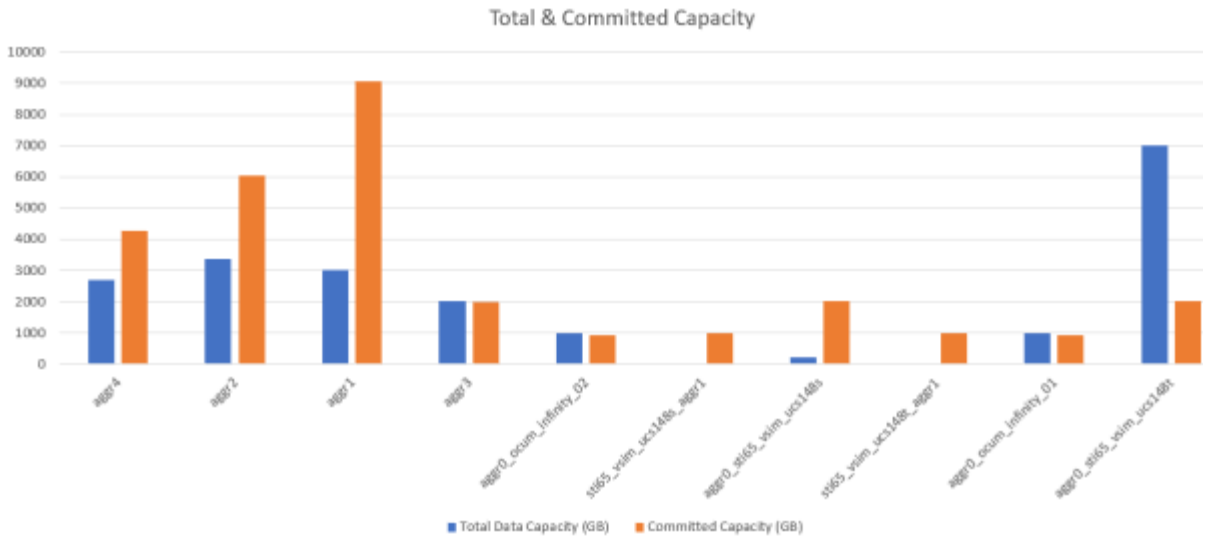
根据您的浏览器，您可能需要单击*确定*以保存文件。

3. 如果需要，请单击*启用编辑*。
4. 在 Excel 中，打开下载的文件。
5. 创建一个新工作表（⊕）在 `data`工作表之后，并将其命名为 总数据容量。
6. 在新的总数据容量表中添加以下列：
   a. 总数据容量（GB）
   b. 已提交的容量（GB）
   c. 已用数据容量（GB）
   d. 可用数据容量（GB）
7. 在每列的第一行输入以下公式，确保它引用数据表（data!），并引用捕获数据的正确列和行说明符（总数据容量从 E 列的第 2 行到第 20 行中提取数据）。
   a. =SUM(data!E$2:data!E$20)
   b. =SUM(data!F$2:data!F$50)
   c. =SUM(data!G$2:data!G$50)
   d. =SUM(data!H$2:data!H$50)

公式将根据当前数据对每列进行汇总。

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. 在数据表中，选择 总数据容量（**GB**） 和 承诺容量（**GB**） 列。
2. 从*插入*菜单中选择*推荐图表*，然后选择*簇状柱形图*。
3. 右键单击图表并选择*移动图表*将图表移动到 `Total Data Capacity`工作表。
4. 使用*设计*和*格式*菜单（在选择图表时可用），您可以自定义图表的外观。
5. 如果满意，请保存包含更改的文件。请勿更改文件名或位置。

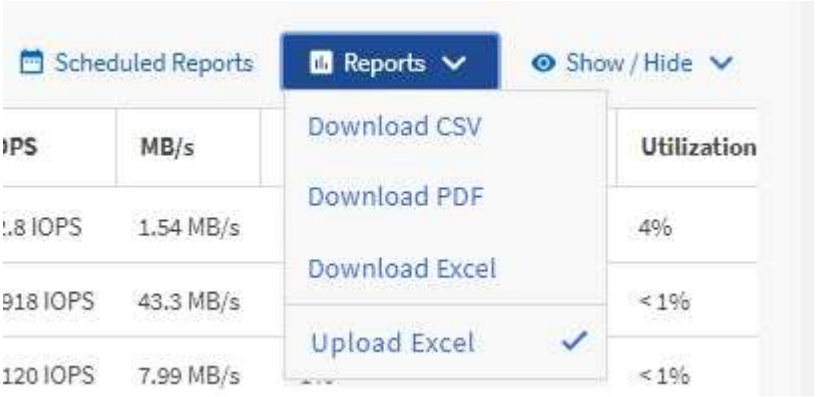


6. 在 Unified Manager 中，选择 报告 > 上传 **Excel**。

   确保您位于下载 Excel 文件的相同视图下。

7. 选择已修改的 Excel 文件。
8. 单击*打开*。
9. 单击*提交*。

   报告 > 上传 **Excel** 菜单项旁边会出现一个复选标记。



10. 单击*已计划报告*。
11. 单击*添加计划*可将新行添加到“报告计划”页面，以便您可以定义新报告的计划特性。

    为报告选择 **XLSX** 格式。

12. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要调查如何最好地利用整个网络中的可用容量。

在 **Active IQ Unified Manager** 中显示聚合总容量与可用容量图表

您可以创建报告，以 Excel 图表格式分析存储总容量和承诺容量。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤打开运行状况：所有聚合视图，在 Excel 中下载视图，创建总容量和承诺容量图表，上传自定义的 Excel 文件，并计划最终报告。

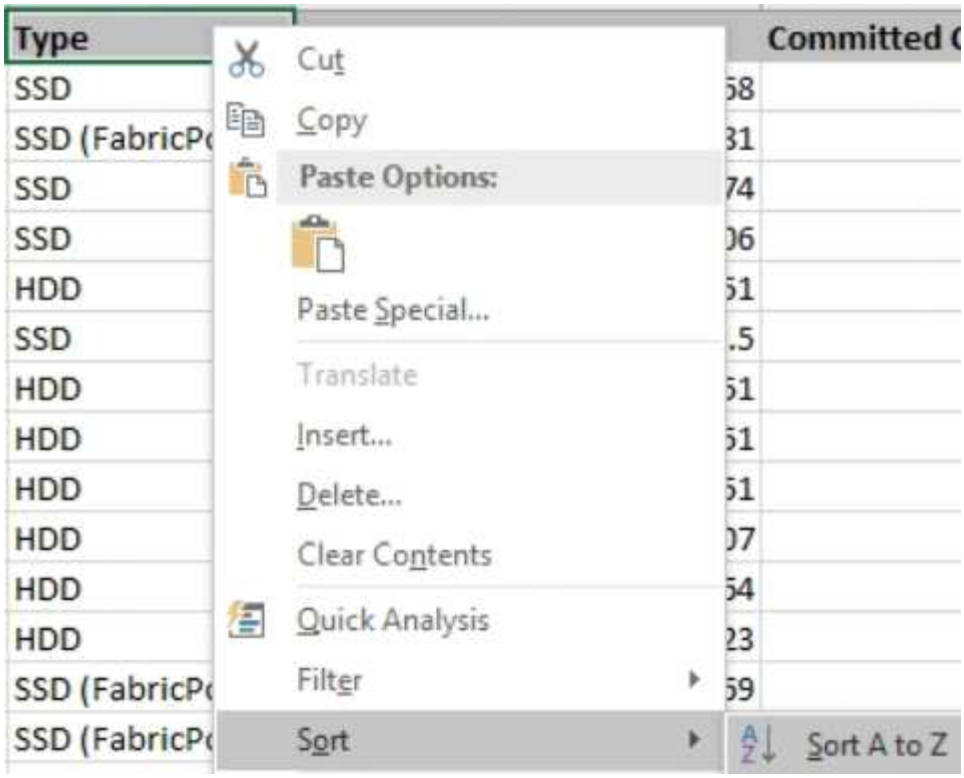
步骤

1. 在左侧导航窗格中，单击*存储* > 聚合。
2. 选择 报告 > 下载 **Excel**。



   根据您的浏览器，您可能需要单击*确定*以保存文件。

3. 在 Excel 中，打开下载的文件。
4. 如果需要，请单击*启用编辑*。
5. 在数据表上，右键单击类型列，然后选择*排序* > 从 **A** 到 **Z** 排序。

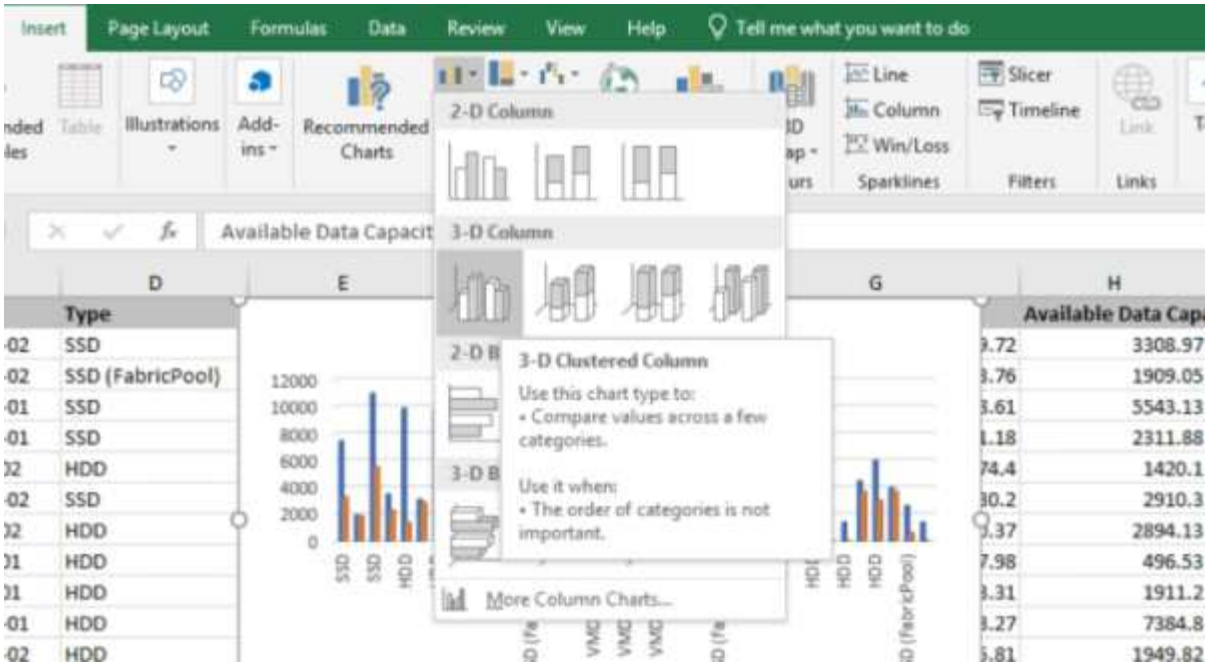


这将按存储类型排列您的数据，例如：

- HDD
- 混合
- SSD
- SSD (FabricPool)

6. 选择 `Type, Total Data Capacity,`和 `Available Data Capacity`列。
7. 在 **Insert** 菜单上，选择一个 `3-D column`图表。

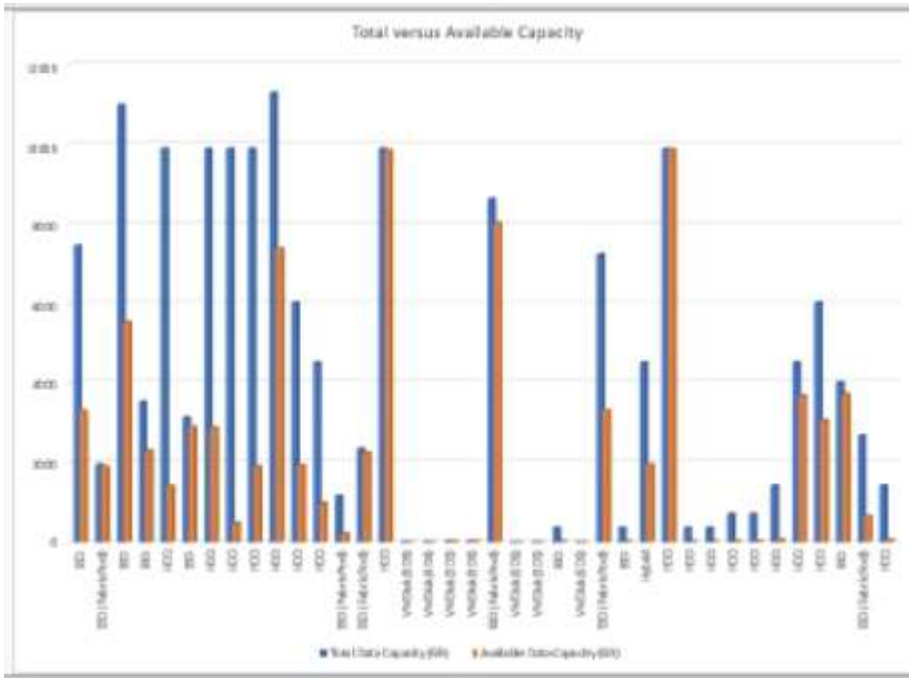
   该图表显示在数据表上。



8. 右键单击图表并选择*移动图表*。
9. 选择*新工作表*并将该工作表命名为*总存储图表*。

   确保新工作表显示在信息和数据表之后。

10. 将图表标题命名为 总容量与可用容量。
11. 使用*设计*和*格式*菜单（在选择图表时可用），您可以自定义图表的外观。
12. 如果满意，请保存包含更改的文件。请勿更改文件名或位置。

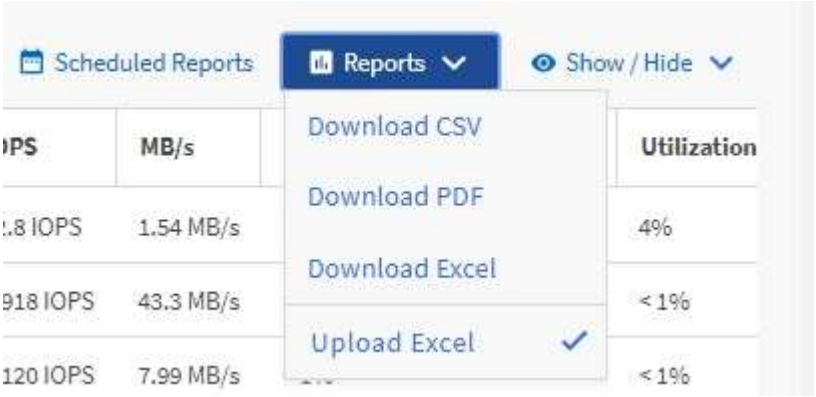


13. 在 Unified Manager 中，选择 报告 > 上传 **Excel**。

确保您位于下载 Excel 文件的相同视图下。

14. 选择已修改的 Excel 文件。
15. 单击*打开*。
16. 单击*提交*。

    报告 > 上传 **Excel** 菜单项旁边会出现一个复选标记。



17. 单击*已计划报告*。
18. 单击*添加计划*可将新行添加到*报告计划*页面，以便您可以定义新报告的计划特性。

    为报告选择 **XLSX** 格式。

19. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能需要平衡聚合上的负载。

创建报告以查看 Active IQ Unified Manager 中的可用卷容量图表

您可以创建报告以分析 Excel 图表中的可用卷容量。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤打开运行状况：所有卷视图，在 Excel 中下载视图，创建可用容量图表，上传自定义的 Excel 文件，并计划最终报告。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 选择 报告 > 下载 **Excel**。



根据您的浏览器，您可能需要单击*确定*以保存文件。

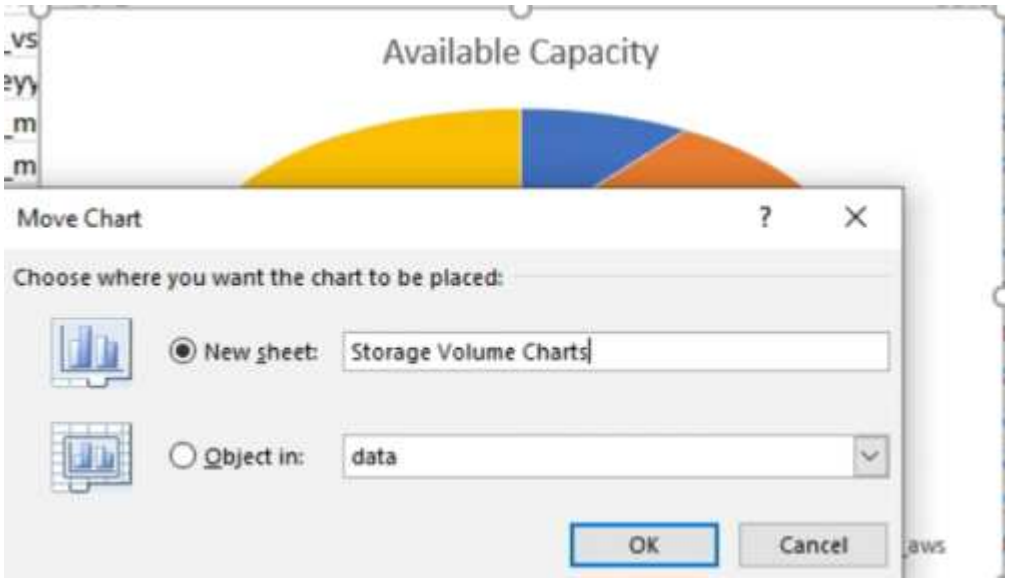
3. 如果需要，请单击*启用编辑*。
4. 在 Excel 中，打开下载的文件。
5. 在 `data`工作表上，选择要在 `Volume`和 `Available Data %` 列中使用的数据。
6. 在 **Insert** 菜单中，选择一个 `3-D piechart.`

   该图表显示哪些卷的可用空间最大。该图表显示在数据表上。

   根据您的网络配置，选择整列或过多的数据行可能会使饼图难以阅读。此示例使用三维饼图，但您可以使用任何图表类型。使用最能显示要捕获的数据的图表。

7. 将图表标题命名为 可用容量。
8. 右键单击图表并选择*移动图表*。
9. 选择*新工作表*并将该工作表命名为*存储卷图表*。

   确保新工作表显示在信息和数据表之后。

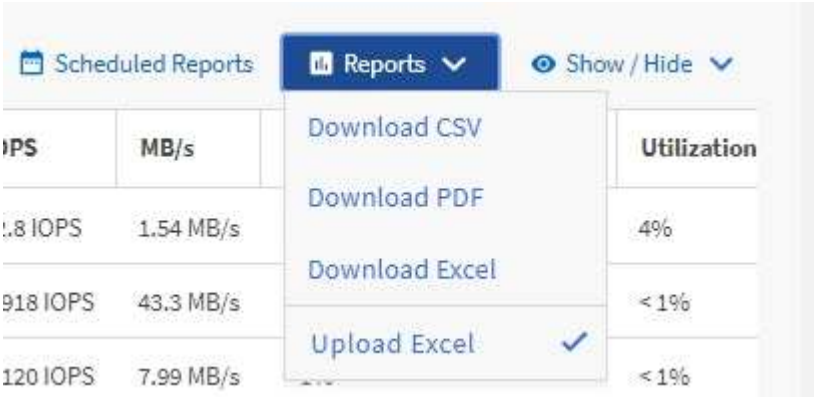


10. 使用*设计*和*格式*菜单（在选择图表时可用），您可以自定义图表的外观。
11. 满意后，保存包含更改的文件。
12. 在 Unified Manager 中，选择 报告 > 上传 **Excel**。

    确保您位于下载 Excel 文件的相同视图下。

13. 选择已修改的 Excel 文件。
14. 单击*打开*。
15. 单击*提交*。

    报告 > 上传 **Excel** 菜单项旁边会出现一个复选标记。



16. 单击*已计划报告*。
17. 单击*添加计划*可将新行添加到*报告计划*页面，以便您可以定义新报告的计划特性。
18. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    为报告选择 **XLSX** 格式。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告显示的结果，您可能需要平衡卷上的负载。

创建报告以查看 Active IQ Unified Manager 中可用 IOPS 最多的聚合

此报表显示每个聚合类型中哪些聚合具有最多的可用 IOPS，您可以在其上配置新工作负载。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤打开运行状况：所有卷视图，在 Excel 中下载视图，创建可用容量图表，上传自定义的 Excel 文件，并计划最终报告。

步骤

1. 在左侧导航窗格中，单击*存储* > 聚合。

2. 从*视图*下拉列表中选择*性能：所有聚合*。
3. 选择*显示/隐藏*以显示 `Available IOPS`列并隐藏 `Cluster FQDN, Inactive Data Reporting,`和 `Threshold Policy`列。
4. 将 `Available IOPS`和 `Free Capacity`列拖放到 `Type`列旁边。
5. 命名并保存自定义视图 `Available IOPS Per Aggr.`
6. 选择 报告 > 下载 **Excel**。



根据您的浏览器，您可能需要单击*确定*以保存文件。

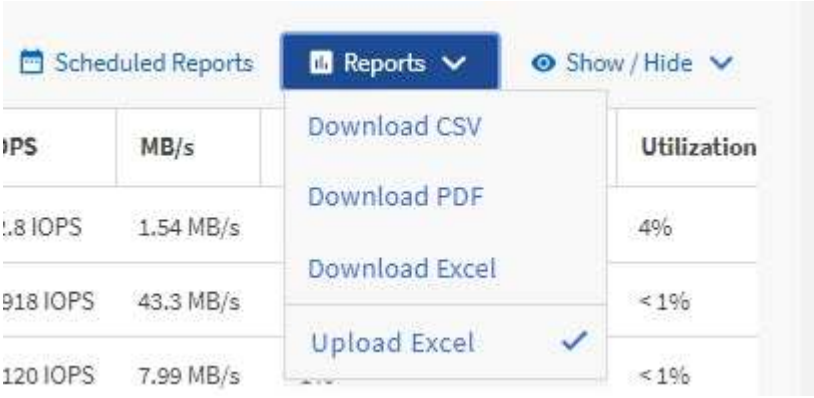
7. 如果需要，请单击*启用编辑*。
8. 在 Excel 中，打开下载的文件。
9. 在数据表上，单击工作表左上角的小三角形以选择整个工作表。
10. 在 数据 功能区上，从 `Sort & Filter area.`选择 排序
11. 设置以下排序级别：
    a. 指定 排序方式 为 `Available IOPS`（IOPS），排序依据 为 `Cell Values,`，顺序 为 `Largest to Smallest.`
    b. 单击*添加级别*。
    c. 指定*排序方式*为 `Type`，*排序依据*为 `Cell Values,`，*顺序*为 `Z to A.`
    d. 单击*添加级别*。
    e. 将*排序方式*指定为 `Free Capacity (GB),`，将*排序依据*指定为 `Cell Values,`，并将*顺序*指定为 `Largest to Smallest.`
    f. 单击 **OK**。
12. 保存并关闭此 Excel 文件。
13. 在 Unified Manager 中，选择 报告 > 上传 **Excel**。

    确保您位于下载 Excel 文件的相同视图下。

14. 选择您已修改的 Excel 文件，在本例中 `performance-aggregates-<date>.xlsx.`

15. 单击*打开*。
16. 单击*提交*。

    报告 > 上传 **Excel** 菜单项旁边会出现一个复选标记。



17. 单击*已计划报告*。
18. 单击*添加计划*可将新行添加到“报告计划”页面，以便您可以定义新报告的计划特性。
19. 输入报告计划的名称并填写其他报告字段，然后单击该行末尾的复选标记（✓）。

    为报告选择 **XLSX** 格式。

    此时将立即发送一个测试报告。之后，此报告将以指定频率生成并通过电子邮件发送给列出的收件人。

根据报告中显示的结果，您可能希望在可用 IOPS 最高的聚合上调配新的工作负载。

使用 REST API 管理存储

Active IQ Unified Manager 入门

Active IQ Unified Manager REST API 入门

Active IQ Unified Manager 提供了一组 API，用于通过 RESTful Web 服务接口管理受支持的存储系统上的存储资源，以便进行任何第三方集成。

在这些主题中，您将找到有关 Unified Manager API、用于解决特定问题的示例工作流和一些示例代码的信息。使用此信息，您可以创建用于管理 NetApp 系统的 NetApp 可管理性软件解决方案的 RESTful 客户端。API 基于 Representational State Transfer （REST） 架构风格。支持所有四个 REST 操作 Create、Read、Update 和 Delete （也称为 CRUD）。

有关 Active IQ Unified Manager REST API 优势的更多资源和详细信息，请参见 "Active IQ Unified Manager"。

确定Active IQ Unified Manager REST API的目标用户

此处的主题适用于创建通过 REST API 与 Active IQ Unified Manager 软件进行交互的应用程序的开发人员。

存储管理员和架构师可以参考此信息，基本了解如何使用 Unified Manager REST API 构建客户端应用程序以管理和监控 NetApp 存储系统。

如果您想使用存储提供程序、ONTAP 集群和管理 API 来管理存储，则应使用此信息。

> 您必须具有以下角色之一：操作员、存储管理员或应用程序管理员。您必须知道要在其上执行 REST API 的 Unified Manager 服务器的 IP 地址或完全限定域名。

管理 Active IQ Unified Manager API 访问权限和类别

Active IQ Unified Manager API 允许您管理和配置环境中的存储对象。您还可以访问 Unified Manager web UI 以执行其中一些功能。

构造 URL 以直接访问 REST API

您可以直接通过编程语言（例如 Python、C#、C++、JavaScript 等）访问 REST API。按以下格式输入主机名或 IP 地址和 URL 以访问 REST API

https://<hostname>/api

> 默认端口为 443。您可以根据环境的要求配置此端口。

访问在线 API 文档页面

您可以访问与产品一起打包的_API 文档_参考内容页面，以显示 API 文档，以及手动发出 API 调用（在界面上，例如 Swagger）。您可以点击*菜单栏* > 帮助按钮 > *API 文档*访问此文档

或者，输入主机名或 IP 地址以及访问 REST API 页面的 URL，格式为

https://<hostname>/docs/api/

类别

API 调用根据区域或类别按功能进行组织。要查找特定 API，请单击适用的 API 类别。

Unified Manager 提供的 REST API 可帮助您执行管理、监控和配置功能。API 分为以下几类。

- 数据中心

  此类别包含帮助您使用 Work Flow Automation 和 Ansible 等工具进行数据中心存储管理和分析的 API。此类别下的 REST API 提供有关数据中心中的集群、节点、聚合、卷、LUN、文件共享、命名空间和其他元素的信息。

- **management-server**

  management-server 类别下的 API 包含 `jobs`， `system`,`和 `events` API。作业是计划用于异步执行的操作，与管理 Unified Manager 上的存储对象或工作负载相关。 `events` API 返回数据中心中的事件，`system` API 返回 Unified Manager 实例详细信息。

- **storage-provider**

  此类别包含管理和调配文件共享、LUN、性能服务级别和存储效率策略所需的所有调配 API。这些 API 还使您能够配置访问端点、Active Directory，以及为存储工作负载分配性能服务级别和存储效率策略。

- 管理

  此类别包含用于运行管理任务的 API，例如维护备份设置、查看 Unified Manager 数据源的信任存储证书以及将 ONTAP 集群作为 Unified Manager 的数据源进行管理。

- 网关

  Unified Manager 使您能够通过网关类别下的 API 调用 ONTAP REST API，并管理数据中心内的存储对象。

- 安全

  此类别包含用于管理 Unified Manager 用户的 API。

了解 **Active IQ Unified Manager** 中提供的 **REST** 服务

在开始使用 Active IQ Unified Manager API 之前，您应该了解所提供的 REST 服务和操作。

用于配置 API 服务器的资源配置和管理 API 支持读取（GET）或写入（POST、PATCH、DELETE）操作。以下是 API 支持的 GET、PATCH、POST 和 DELETE 操作的一些示例：

- GET 示例： `GET /datacenter/cluster/clusters` 检索数据中心中的集群详细信息。 `GET` 操作返回的最大记录数为 1000。

  API 使您能够按支持的属性对记录进行筛选、排序和排列。

- POST 示例： `POST /datacenter/svm/svms` 创建自定义 Storage Virtual Machine (SVM)。
- PATCH 示例： `PATCH /datacenter/svm/svms/{key}` 使用其唯一键修改 SVM 的属性。
- DELETE 示例： `DELETE /storage-provider/access-endpoints/{key}` 使用其唯一密钥从 LUN 、SVM 或文件共享中删除访问端点。

可以使用 API 执行的 REST 操作取决于操作员、存储管理员或应用程序管理员用户的角色。

用户角色	支持的 **REST** 方法
运算符	对数据的只读访问。具有此角色的用户可以运行所有 GET 请求。
存储管理员	对所有数据的读取访问权限。具有此角色的用户可以运行所有 GET 请求。 此外，他们还具有写入权限（运行 PATCH、POST 和 DELETE 请求），以执行特定活动，例如管理、存储服务对象和存储管理选项。
应用程序管理员	对所有数据的读写访问权限。具有此角色的用户可以对所有功能运行 GET、PATCH、POST 和 DELETE 请求。

有关所有 REST 操作的详细信息，请参见_在线 API 文档_。

了解 **Active IQ Unified Manager** 中的 **API** 版本号

Active IQ Unified Manager 中的 REST API URI 指定了一个版本号。例如， `/v2/datacenter/svm/svms`. 其中版本号 `v2` 位于 `/v2/datacenter/svm/svms` 中，表示特定版本中使用的 API 版本。版本号通过返回客户端可以处理的响应，最大程度地减少 API 更改对客户端软件的影响。

此版本号的数字部分相对于各个版本是递增的。带有版本号的 URI 提供了一致的接口，可在未来的版本中保持向后兼容性。您还可以找到没有版本的相同 API，例如 `/datacenter/svm/svms,`，这表示没有版本的基本 API。基本 API 始终是最新版本的 API。

在 Swagger 界面的右上角，您可以选择要使用的 API 版本。默认情况下选择最高版本。建议您使用 Unified Manager 实例中可用的特定 API 的最高版本（相对于增量整数）。

对于所有请求，您必须明确指定要使用的 API 版本。指定版本号后，服务将不会返回您的应用程序无法处理的响应元素。在 REST 请求中，您应包含版本参数。API 的早期版本最终将在几个版本发布后被弃用。在此版本中， `v1` 版本的 API 已被弃用。

了解 **Active IQ Unified Manager** 中的 **ONTAP** 存储资源模型

ONTAP 中的存储资源可大致分为_物理存储资源_和_逻辑存储资源。_要使用 Active IQ Unified Manager 中提供的 API 有效管理您的 ONTAP 系统，您必须了解存储资源模型以及各种存储资源之间的关系。

- 物理存储资源

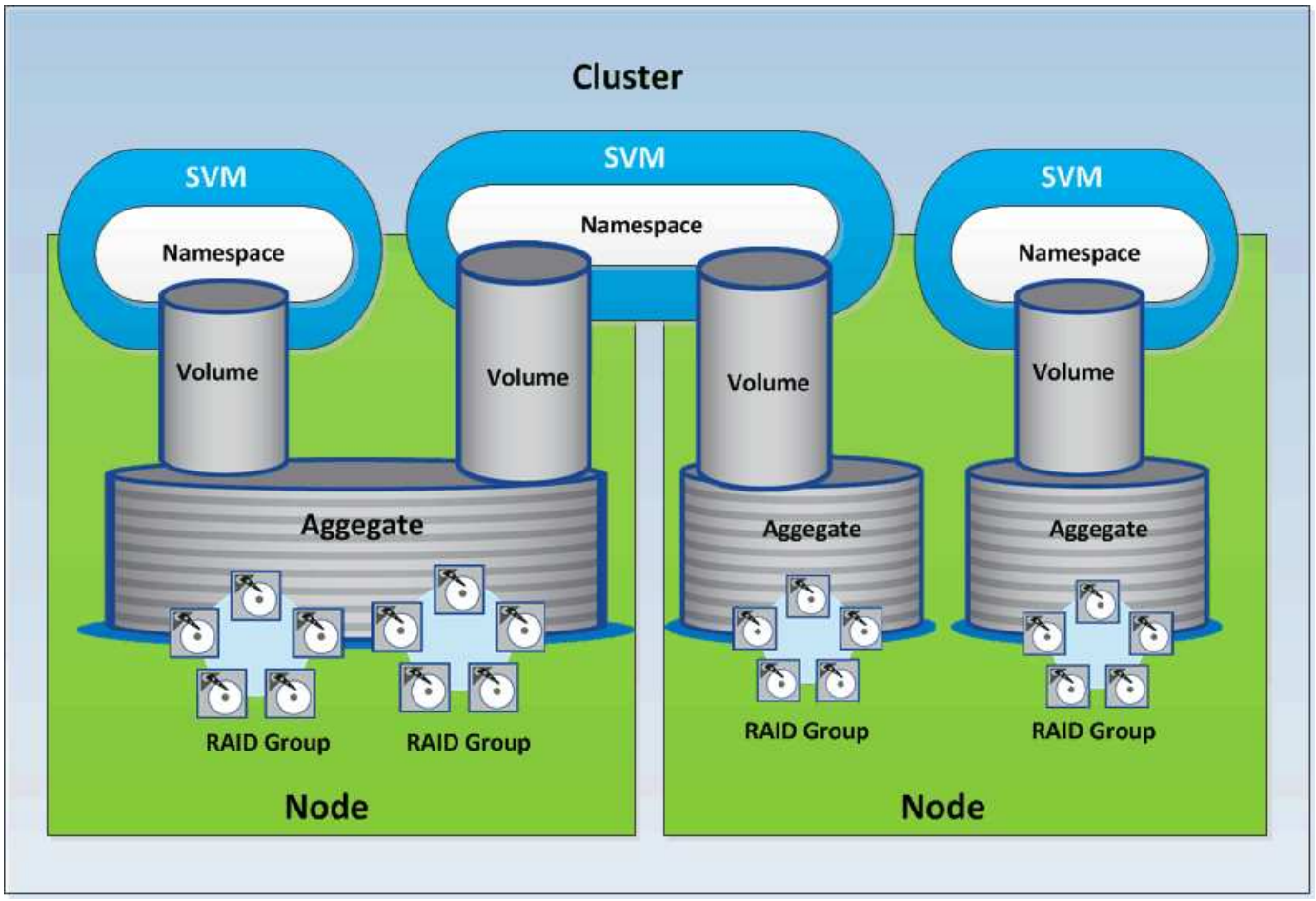
指 ONTAP 提供的物理存储对象。物理存储资源包括磁盘、集群、存储控制器、节点和聚合。

- 逻辑存储资源

  指 ONTAP 提供的、不与物理资源绑定的存储资源。这些资源与Storage Virtual Machine（SVM，以前称为 Vserver）关联，独立于任何特定的物理存储资源（如磁盘、阵列 LUN 或聚合）而存在。

  逻辑存储资源包括所有类型的卷和 qtree，以及可用于这些资源的功能和配置，例如 Snapshot 副本、重复数据删除、数据压缩和配额。

下图显示了 2 节点集群中的存储资源：



Active IQ Unified Manager 中的 REST API 访问和身份验证

在 Active IQ Unified Manager 中访问和验证 REST API

可以使用任何能够通过基本 HTTP 身份验证机制发出 HTTP 请求的 REST 客户端或编程平台来访问 Active IQ Unified Manager REST API。

请求和响应示例：

- 请求

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

- 响应

```
{
  "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* 是 API 服务器的 IP 地址或完全限定的域名（FQDN）。
- 端口 443

443 是默认的 HTTPS 端口。如果需要，您可以自定义 HTTPS 端口。

要从 Web 浏览器发出 HTTP 请求，您必须使用 REST API 浏览器插件。您还可以使用脚本平台（如 cURL

和 Perl）访问 REST API。

身份验证

Unified Manager 支持 API 的基本 HTTP 身份验证方案。为了确保信息流（请求和响应）的安全，REST API 只能通过 HTTPS 访问。API 服务器向所有客户端提供自签名 SSL 证书以进行服务器验证。此证书可由自定义证书（或 CA 证书）替换。

必须配置用户对 API 服务器的访问权限以调用 REST API。用户可以是本地用户（存储在本地数据库中的用户配置文件）或 LDAP 用户（如果已将 API 服务器配置为通过 LDAP 进行身份验证）。您可以通过登录到 Unified Manager 管理控制台用户界面来管理用户访问。

了解 **Active IQ Unified Manager HTTP** 状态代码

在运行 API 或排除问题时，应注意 Active IQ Unified Manager API 使用的各种 HTTP 状态代码和错误代码。

下表列出了与身份验证相关的错误代码：

HTTP 状态代码	状态代码标题	问题描述
200	确定	成功执行同步 API 调用时返回。
201	已创建	通过同步调用创建新资源，例如配置 Active Directory。
202	已接受	成功执行配置功能的异步调用时返回，例如创建 LUN 和文件共享。
400	无效请求	表示输入验证失败。用户必须更正输入，例如请求正文中的有效键。
401	未经授权的请求	您无权查看资源/未授权。
403	禁止的请求	禁止访问您尝试访问的资源。
404	未找到资源	未找到您尝试访问的资源。
405	方法不允许	方法不允许。
429	请求过多	当用户在特定时间内发送太多请求时返回。
500	内部服务器错误	内部服务器错误。无法从服务器获取响应。此内部服务器错误可能是也可能不是永久性的。例如，如果您运行 `GET`或 `GET ALL`操作并收到此错误，建议您至少重试此操作五次。如果是永久性错误，则返回的状态代码仍为 500。如果操作成功，则返回的状态代码为 200。

请遵循使用 **Active IQ Unified Manager API** 的推荐做法

在 Active IQ Unified Manager 中使用 API 时，应遵循某些推荐做法。

- 所有响应内容类型必须采用以下格式才能有效执行：

```
application/json
```

- API 版本号与产品版本号无关。您应使用适用于您的 Unified Manager 实例的最新可用 API 版本。有关 Unified Manager API 版本的详细信息，请参见“`REST API versioning in Active IQ Unified Manager`”部分。
- 在使用 Unified Manager API 更新数组值时，您必须更新整个值字符串。您不能向数组附加值。您只能替换现有的数组。
- 您可以对所有查询参数使用筛选器运算符，例如管道（|）和通配符（*），但双精度值（例如指标 API 中的 IOPS 和性能）除外。
- 避免使用过滤器运算符通配符（*）和管道（|）的组合来查询对象。这可能会检索到数量不正确的对象。
- 使用筛选器值时，请确保此值不包含任何 `?`字符。这是为了降低 SQL 注入的风险。
- 请注意，任何 API 的 `GET` （all）请求最多返回 1000 条记录。即使通过将 `max_records` 参数设置为大于 1000 的值来运行查询，也只会返回 1000 条记录。
- 要执行管理功能，建议使用 Unified Manager UI。

使用 **Active IQ Unified Manager** 中的系统日志进行故障排除

系统日志可用于分析运行 API 时可能出现的故障原因和故障排除问题。

从以下位置检索日志，以解决与 API 调用相关的问题。

日志位置	用途
`/var/log/ocie/access_log.log`	包含所有 API 调用详细信息，例如调用 API 的用户的用户名、开始时间、执行时间、状态和 URL。 您可以使用此日志文件检查常用 API，或对任何 GUI 工作流进行故障排除。您还可以根据执行时间使用它进行缩放分析。
`/var/log/ocum/ocumserver.log`	包含所有 API 执行日志。 您可以使用此日志文件对 API 调用进行故障排除和调试。
`/var/log/ocie/server.log`	包含所有 Wildfly 服务器部署和启动/停止服务相关日志。 您可以使用此日志文件查找在 Wildfly 服务器的启动、停止或部署期间发生的任何问题的根本原因。
`/var/log/ocie/au.log`	包含与采集单元相关的日志。 当您在 ONTAP 中创建、修改或删除了任何对象，但它们未反映在 Active IQ Unified Manager REST API 中时，您可以使用此日志文件。

了解 **Active IQ Unified Manager** 如何使用作业对象进行异步处理

Active IQ Unified Manager 提供了 `jobs` API，用于检索有关在运行其他 API 时执行的作业的信息。您必须了解如何使用作业对象进行异步处理。

某些 API 调用，特别是用于添加或修改资源的 API 调用，可能需要比其他调用更长的时间才能完成。Unified Manager 异步处理这些长期运行的请求。

使用 **Job** 对象描述的异步请求

在进行异步运行的 API 调用后，HTTP 响应代码 202 表示请求已成功验证和接受，但尚未完成。此请求作为后台任务处理，此后台任务在对客户端的初始 HTTP 响应后继续运行。响应包括锚定请求的 Job 对象，包括其唯一标识符。

查询与 **API** 请求关联的作业对象

HTTP 响应中返回的 Job 对象包含多个属性。您可以查询 state 属性以确定请求是否成功完成。Job 对象可以处于以下状态之一：

- `NORMAL`
- `WARNING`
- `PARTIAL_FAILURES`
- `ERROR`

在轮询 Job 对象以检测任务的终端状态时，您可以使用两种技术，无论是成功还是失败：

- 标准轮询请求：立即返回当前作业状态。
- 长轮询请求：当作业状态变为 `NORMAL`, `ERROR`,`或 `PARTIAL_FAILURES.

异步请求中的步骤

您可以使用以下高级过程完成异步 API 调用：

1. 发出异步 API 调用。
2. 接收 HTTP 响应 202，指示成功接受请求。
3. 从响应正文中提取 Job 对象的标识符。
4. 在循环中，等待 Job 对象到达终止状态 `NORMAL`, `ERROR`,`或 `PARTIAL_FAILURES.
5. 验证作业的最终状态并获取作业结果。

了解 **Active IQ Unified Manager** 中的 **Hello API server** 示例程序

Hello API server 是一个示例程序，演示了如何使用简单的 REST 客户端在 Active IQ Unified Manager 中调用 REST API。该示例程序以 JSON 格式（服务器仅支持 `application/json`格式）为您提供有关 API 服务器的基本详细信息。

使用的 URI 为： `https://<hostname>/api/datacenter/svm/svms.`此示例代码采用以下输入参数：

- API 服务器 IP 地址或 FQDN
- 可选：端口号（默认：443）
- 用户名
- 密码
- 响应格式 (`application/json`)

要调用 REST API，您还可以使用其他脚本（如 Jersey 和 RESTEasy）为 Active IQ Unified Manager 编写 Java REST 客户端。您应该了解有关示例代码的以下注意事项：

- 使用到 Active IQ Unified Manager 的 HTTPS 连接来调用指定的 REST URI
- 忽略 Active IQ Unified Manager 提供的证书
- 在握手过程中跳过主机名验证
- 使用 `javax.net.ssl.HttpsURLConnection`进行 URI 连接
- 使用第三方库(`org.apache.commons.codec.binary.Base64`）构造 HTTP 基本身份验证中使用的 Base64 编码字符串

要编译和执行示例代码，您必须使用 Java 编译器 1.8 或更高版本。

```
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;
    }

}
```

Unified Manager REST API

了解 **Active IQ Unified Manager REST API** 的类别

本节根据类别列出了 Active IQ Unified Manager 的 REST API。

您可以从 Unified Manager 实例查看在线文档页面，其中包含每个 REST API 调用的详细信息。本文档不重复在线文档的详细信息。本文档中列出或描述的每个 API 调用仅包含您在文档页面上查找调用所需的信息。找到特定 API 调用后，您可以查看该调用的完整详细信息，包括输入参数、输出格式、HTTP 状态代码和请求处理类型。

工作流程中每个 API 调用都包含以下信息，以帮助在文档页面上查找该调用：

- 类别

  API 调用在文档页面上组织成与功能相关的区域或类别。要查找特定 API 调用，请向下滚动到页面底部，然后单击适用的 API 类别。

- HTTP 动词（调用）

  HTTP 谓词标识对资源执行的操作。每个 API 调用都通过单个 HTTP 谓词执行。

- 路径

  路径确定操作在执行调用时使用的特定资源。路径字符串附加到核心 URL，以形成标识资源的完整 URL。

使用 **Active IQ Unified Manager** 中的 **API** 管理数据中心中的存储对象

`datacenter` 类别下的 REST API 使您能够管理数据中心中的存储对象，例如集群、节点、聚合、存储 VM、卷、LUN、文件共享和命名空间。这些 API 可用于查询对象的配置，而其中一些 API 可让您执行添加、删除或修改这些对象的操作。

这些 API 大多数是 GET 调用，可通过过滤、排序和分页支持提供跨集群聚合。在运行这些 API 时，它们会从数据库中返回数据。因此，新创建的对象需要在下一个采集周期中被发现才能出现在响应中。

如果要查询特定对象的详细信息，则需要输入该对象的唯一 ID 才能查看其详细信息。例如，有关存储对象的指标和分析信息，请参阅 "查看性能指标"。

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

CURL 命令、示例、请求和对 API 的响应可在您的 Swagger API 界面上找到。您可以按照 Swagger 上指示的特定参数对结果进行筛选和排序。这些 API 使您能够筛选特定存储对象（如集群、卷或存储 VM）的结果。

数据中心存储对象的 **API**

HTTP 谓词	路径	问题描述
GET	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}	您可以使用此方法查看整个数据中心的 ONTAP 集群详细信息。该 API 返回信息，例如集群的 IPv4 或 IPv6 地址、有关节点的信息，例如节点健康状况、性能容量和高可用性（HA）对，并指示集群是否为 All SAN Array。

HTTP 谓词	路径	问题描述
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	返回安装在数据中心集群上的许可证的详细信息。您可以根据所需条件筛选结果。将返回许可证密钥、集群密钥、到期日期和许可证范围等信息。您可以输入许可证密钥以检索特定许可证的详细信息。
GET	/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}	您可以使用此方法查看数据中心中节点的详细信息。您可以查看有关该节点的集群、节点运行状况、性能容量和高可用性（HA）对的信息。
GET	/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}	您可以使用此方法查看数据中心中 CIFS 共享的详细信息。除了集群、SVM 和卷详细信息外，还会返回有关访问控制列表（ACL）的信息。
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	您可以使用此方法查看受支持的 NFS 服务的导出策略详细信息。 您可以查询集群或存储虚拟机的导出策略，并重用导出策略密钥来配置 NFS 文件共享。有关在工作负载上分配和重用导出策略的详细信息，请参见“配置 CIFS 和 NFS 文件共享”。
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	您可以使用此方法查看数据中心内的聚合集合或特定聚合，以便在其上调配工作负载或进行监控。将返回集群和节点详细信息、已用性能容量、可用和已用空间以及存储效率等信息。
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	您可以使用此方法查看整个数据中心中的 LUN 集合。您可以查看有关 LUN 的信息，例如群集和 SVM 详细信息、QoS 策略和 igroup。
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	您可以使用此方法查看适用于数据中心内存储对象的所有 QoS 策略的详细信息。将返回集群和 SVM 详细信息、固定或自适应策略详细信息以及适用于该策略的对象数量等信息。
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	您可以使用此方法查看整个数据中心内所有 FlexVol 卷或 FlexGroup 卷的 qtree 详细信息。将返回集群和 SVM 详细信息、FlexVol 卷以及导出策略等信息。

HTTP 谓词	路径	问题描述
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	您可以使用此方法查看数据中心中的卷集合。返回有关卷的信息，例如 SVM 和集群详细信息、QoS 和导出策略，以及卷是读写类型、数据保护类型还是负载共享类型。 对于 FlexVol 和 FlexClone 卷，您可以查看有关相应聚合的信息。对于 FlexGroup 卷，查询将返回组成聚合的列表。
GET POST DELETE PATCH	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}	您可以分配授权访问特定 LUN 目标的启动程序组（igroup）。如果存在现有的 igroup，您可以分配它。您还可以创建 igroup 并将其分配给 LUN。 您可以使用这些方法分别查询、创建、删除和修改 igroup。 注意事项： • POST：创建 igroup 时，您可以指定要分配访问权限的存储虚拟机。 • DELETE：要删除特定的 igroup，需要提供 igroup 键作为输入参数。如果已将 igroup 分配给 LUN，则无法删除该 igroup。 • PATCH：您需要提供 igroup 键作为输入参数来修改特定的 igroup。您还必须输入要更新的属性及其值。
GET POST DELETE PATCH	/datacenter/svm/svms /datacenter/svm/svms/{key}	您可以使用这些方法来查看、创建、删除和修改 Storage Virtual Machines（存储 VM）。 • POST：您必须输入要创建的存储 VM 对象作为输入参数。您可以创建自定义存储 VM，然后为其分配所需的属性。 • DELETE：您需要提供存储 VM 密钥才能删除特定存储 VM。 • PATCH：您需要提供 storage VM 密钥才能修改特定的 storage VM。您还需要输入要更新的属性及其值。

注意事项：

如果在环境中启用了基于 SLO 的工作负载配置，在创建存储 VM 时，请确保它支持在其上配置 LUN 和文件共享所需的所有协议，例如 CIFS 或 SMB、NFS、FCP 和 iSCSI。如果存储 VM 不支持所需的服务，则配置工作流可能会失败。建议在存储 VM 上也启用相应类型工作负载的服务。

如果您在环境中启用了基于 SLO 的工作负载调配，则无法删除在其上调配了存储工作负载的存储虚拟机。当您删除配置了 CIFS 或 SMB 服务器的存储虚拟机时，此 API 还会删除 CIFS 或 SMB 服务器以及本地 Active Directory 配置。但是，CIFS 或 SMB 服务器名称仍然位于 Active Directory 配置中，您必须从 Active Directory 服务器手动将其删除。

数据中心网络元素的 **API**

数据中心类别中的以下 API 检索有关环境中端口和网络接口的信息，特别是 FC 端口、FC 接口、以太网端口和 IP 接口。

HTTP 谓词	路径	问题描述

`GET`	`/datacenter/network/ethernet/ports`
	
	`/datacenter/network/ethernet/ports/{key}`
		检索数据中心环境中所有以太网端口的相关信息。以端口密钥作为输入参数，您可以查看该特定端口的信息。系统将检索相关信息，例如集群详细信息、广播域、端口详细信息（如状态、速度和类型），以及端口是否已启用。

`GET`	`/datacenter/network/fc/interfaces`
	
	`/datacenter/network/fc/interfaces/{key}`
		您可以使用此方法查看数据中心环境中 FC 接口的详细信息。使用接口键作为输入参数，您可以查看该特定接口的信息。将检索集群详细信息、主节点详细信息和主端口详细信息等信息。

`GET`	`/datacenter/network/fc/ports`
	
	`/datacenter/network/fc/ports/{key}`
		检索有关数据中心环境中节点所使用的所有 FC 端口的信息。使用端口键作为输入参数，您可以查看该特定端口的信息。将检索集群详细信息、端口描述、支持的协议和端口状态等信息。

`GET`	`/datacenter/network/ip/interfaces`
	
	`/datacenter/network/ip/interfaces/{key}`
		您可以使用此方法查看数据中心环境中 IP 接口的详细信息。将接口键作为输入参数，您可以查看该特定接口的信息。将检索集群详细信息、IPspace 详细信息、主节点详细信息以及是否启用故障转移等信息。

通过 **Active IQ Unified Manager** 中的代理访问来访问 **ONTAP API**

网关 API 为您提供了使用 Active IQ Unified Manager 凭据运行 ONTAP REST API 和管理存储对象的优势。当从 Unified Manager Web UI 启用 API 网关功能时，这些 API 可用。

Unified Manager REST API 仅支持对 Unified Manager 数据源（即 ONTAP 群集）执行的一组选定操作。您可以通过 ONTAP API 使用其他功能。网关 API 允许 Unified Manager 作为直通接口，用于隧道传输要在其管理的 ONTAP 群集上执行的所有 API 请求，而无需单独登录到每个数据中心群集。它充当单点管理，用于在由您的

Unified Manager 实例管理的 ONTAP 群集上运行 API。API 网关功能允许 Unified Manager 作为单个控制平面，您可以从中管理多个 ONTAP 群集，而无需单独登录到这些群集。网关 API 使您能够保持登录到 Unified Manager，并通过运行 ONTAP REST API 操作来管理 ONTAP 群集。

所有用户都可以使用 GET 操作运行查询。应用程序管理员可以运行所有 ONTAP REST 操作。

网关充当代理，通过保持与 ONTAP API 相同格式的标头和正文请求来建立 API 请求隧道。您可以使用 Unified Manager 凭据并执行特定操作来访问和管理 ONTAP 集群，而无需传递各个集群的凭据。它继续管理集群身份验证和集群管理，但会将 API 请求重定向为直接在特定集群上运行。API 返回的响应与直接从 ONTAP 执行的相应 ONTAP REST API 返回的响应相同。

HTTP 谓词	路径（**URL**）	问题描述
`GET`	`/gateways`	此 GET 方法检索由 Unified Manager 管理的支持 ONTAP REST 调用的所有集群的列表。您可以验证集群详细信息，并选择基于集群 UUID 或通用唯一标识符（UUID）运行其他方法。 网关 API 仅检索 ONTAP 9.5 或更高版本支持，并通过 HTTPS 添加到 Unified Manager 的集群。

`GET`
`POST`
`DELETE`
`PATCH`
`OPTIONS` （不适用于 Swagger）
`HEAD` （在 Swagger 上不可用）
	`/gateways/{uuid}/{path}`
	{uuid} 的值必须替换为要对其执行 REST 操作的集群 UUID。此外，请确保 UUID 属于 ONTAP 9.5 或更高版本支持的集群，并已通过 HTTPS 添加到 Unified Manager。{path} 必须替换为 ONTAP REST URL。您必须从 URL 中删除 `/api/`。
		这是一个单点代理 API，支持所有 ONTAP REST API 的 POST、DELETE、PATCH 操作和 GET。只要 ONTAP 支持，对任何 API 都没有限制。无法禁用隧道或代理功能。
		此 `OPTIONS` 方法返回 ONTAP REST API 支持的所有操作。例如，如果 ONTAP API 仅支持 `GET` 操作，则使用此网关 API 运行 `OPTIONS` 方法将返回 `GET` 作为响应。Swagger 不支持此方法，但可以在其他 API 工具上执行。
		此 `OPTIONS`方法确定资源是否可用。此操作可用于查看 HTTP 响应标头中有关资源的元数据。Swagger 不支持此方法，但可以在其他 API 工具上执行。

了解 **API** 网关隧道

网关 API 使您能够通过 Unified Manager 管理 ONTAP 对象。Unified Manager 管理集群和身份验证详细信息，并将请求重定向到 ONTAP REST 端点。网关 API 使用 API 网关基础 URL 转换标头和响应正文中的 URL 和作为应用程序状态引擎的超媒体（HATEOAS）链接。网关 API 充当代理基础 URL，您可以向其附加 ONTAP

REST URL 并执行所需的 ONTAP REST 端点。

> 要使 ONTAP API 通过 API 网关成功运行，运行该 API 的 ONTAP 群集版本必须支持该 API。运行 ONTAP 群集不支持的 API 不会返回任何结果。

在此示例中，网关 API（代理基 URL）为： `/gateways/{uuid}/`

所采用的 ONTAP API 为： `/storage/volumes`。您需要将 ONTAP API REST URL 添加为 path 参数的值。

> 添加路径时，请确保已删除"`/" symbol at the beginning of the URL. For the API `/storage/volumes`, add `storage/volumes`.

附加的 URL 是： `/gateways/{uuid}/storage/volumes`

运行 `GET`操作时，生成的 `URL` 如下所示：
`GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes`

在附加的 URL 中删除了 ONTAP REST URL 的 `/api`标签，并保留了网关 API 的标签。

示例 **cURL** 命令

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes" -H "accept: application/hal+json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

API 返回该集群中的存储卷列表。响应格式与从 ONTAP 运行相同 API 时收到的格式相同。返回的状态代码是 ONTAP REST 状态代码。

设置 **API** 范围

所有 API 都具有在集群范围内设置的上下文。基于存储 VM 运行的 API 也以集群为范围，即在托管集群内的特定存储 VM 上执行 API 操作。运行 `/gateways/{uuid}/{path}` API 时，请确保输入运行操作的集群的集群 UUID（Unified Manager 数据源 UUID）。要将上下文设置为该集群中的特定存储 VM，请输入存储 VM 密钥作为 X-Dot-SVM-UUID 参数，或输入存储 VM 名称作为 X-Dot-SVM-Name 参数。该参数作为筛选器添加到字符串标头中，操作在该集群内的该存储 VM 范围内运行。

示例 **cURL** 命令

```
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>"
```

有关使用 ONTAP REST API 的详细信息，请参见 "ONTAP REST API 自动化"

使用 **Active IQ Unified Manager** 中的 **API** 执行管理任务

您可以使用 `administration`类别下的 API 修改备份设置、验证备份文件信息和集群证书，还可以将 ONTAP 集群作为 Active IQ Unified Manager 数据源进行管理。

要运行这些操作，您必须具有应用程序管理员角色。您还可以使用 Unified Manager Web UI 配置这些设置。

HTTP 谓词	路径	问题描述

`GET`
 	
`PATCH`
	`/admin/backup-settings`
	
	`/admin/backup-settings`
		您可以使用 `GET` 方法查看默认情况下在 Unified Manager 中配置的备份计划的设置。您可以验证以下信息：
		
		• 计划是否已启用或禁用
		• 计划备份的频率（每日或每周）
		• 备份时间
		• 应用程序中应保留的最大备份文件数
		
		备份时间采用服务器时区。
		
		默认情况下，数据库备份设置在 Unified Manager 上可用，您无法创建备份计划。但是，您可以使用 `PATCH` 方法修改默认设置。

`GET`	`/admin/backup-file-info`	每次为 Unified Manager 修改备份计划时，都会生成一个备份转储文件。您可以使用此方法验证备份文件是否根据修改后的备份设置生成，以及文件上的信息是否与修改后的设置匹配。
`GET`	`/admin/datasource-certificate`	可以使用此方法从信任存储查看数据源（群集）证书。在将 ONTAP 群集添加为 Unified Manager 数据源之前，需要验证证书。

`GET`
 	
`POST`
 	
`PATCH`
 	
`DELETE`
	`/admin/datasources/clusters`
	
	`/admin/datasources/clusters/{key}`
		您可以使用 `GET`方法检索由 Unified Manager 管理的数据源（ONTAP 群集）的详细信息。
		
		您还可以将新集群作为数据源添加到 Unified Manager。要添加集群，您必须知道其主机名、用户名和密码。
		
		要修改和删除由 Unified Manager 作为数据源管理的集群，请使用 ONTAP 集群密钥。

使用 API 管理 Active IQ Unified Manager 中的用户

您可以使用 `security` 类别中的 API 来控制用户对 Active IQ Unified Manager 中选定集群对象的访问。您可以添加本地用户或数据库用户。您还可以添加属于身份验证服务器的远程用户或组。根据您分配给用户的角色的权限，他们可以管理存储对象或查看 Unified Manager 中的数据。

要运行这些操作，您必须具有应用程序管理员角色。您还可以使用 Unified Manager Web UI 配置这些设置。

`security` 类别下的 API 使用 `users` 参数（即用户名），而不是 `key` 参数作为用户实体的唯一标识符。

HTTP 谓词	路径	问题描述

`GET`
 	
`POST`
	`/security/users`
	
	`/security/users`
		您可以使用这些方法获取用户的详细信息或将新用户添加到 Unified Manager。
		
		您可以根据用户类型向用户添加特定角色。添加用户时，必须提供本地用户、维护用户和数据库用户的密码。

`GET`
 	
`PATCH`
 	
`DELETE`
	`/security/users/{name}`	使用 GET 方法，您可以检索用户的所有详细信息，例如名称、电子邮件地址、角色、授权类型。使用 PATCH 方法，您可以更新详细信息。使用 DELETE 方法，您可以删除用户。

使用 Active IQ Unified Manager 中的 API 查看性能指标

Active IQ Unified Manager 为您提供了一组 `/datacenter` 类别下的 API，使您能够查看数据中心中集群和存储对象的性能数据。这些 API 检索不同存储对象的性能数据，如集群、节点、LUN、卷、聚合、存储 VM、FC 接口、FC 端口、以太网端口和 IP 接口。

`/metrics` 和 `/analytics` API 提供了性能指标的不同视图，使用这些视图，您可以深入了解数据中心内以下存储对象的不同详细级别：

- 集群
- nodes
- 存储 VM
- 聚合

- volumes
- LUN 数
- FC 接口
- FC 端口
- 以太网端口
- IP 接口

下表就检索到的性能数据详细信息对 `/metrics` 和 `/analytics` API 进行了比较。

指标	分析
单个对象的性能详细信息。例如，`/datacenter/cluster/clusters/{key}/metrics` API 要求输入集群键作为路径参数，以便检索该特定集群的指标。	数据中心中相同类型的多个对象的性能详细信息。例如，`/datacenter/cluster/clusters/analytics` API 检索数据中心中所有集群的集体指标。
基于用于检索的时间间隔参数的存储对象的性能指标示例。	特定类型存储对象在一定时间段（72 小时以上）内性能的高级聚合值。
将检索对象的基本详细信息，例如节点或集群的详细信息。	未检索到任何具体详细信息。
检索单个对象的累积计数器（例如最小值、最大值、第 95 个百分位数以及一段时间内的平均性能值），例如读取、写入、总计和其他计数器。	相同类型的所有对象都显示单个聚合值。

指标	分析
时间范围和样本数据基于以下计划：数据的时间范围。示例可以是 1h、12h、1d、2d、3d、15d、1w、1m、2m、3m、6m。如果范围超过 3 天（72 小时），则获得 1 小时样本，否则为 5 分钟样本。每个时间范围的周期如下： • 1 小时：在 5 分钟内采样的最近一小时的指标。 • 12h：最近 12 小时的指标，每 5 分钟采样一次。 • 1d：最近一天的指标，采样间隔为 5 分钟。 • 2d：最近 2 天的指标，每 5 分钟采样一次。 • 3d：最近 3 天的指标，采样间隔为 5 分钟。 • 15d：最近 15 天的指标，按 1 小时采样。 • 1w：最近一周的指标，按 1 小时采样。 • 1m：最近一个月的指标，采样间隔为 1 小时。 • 2m：最近 2 个月的指标，按 1 小时进行采样。 • 3m：最近 3 个月的指标，采样间隔为 1 小时。 • 6m：最近 6 个月的指标，采样间隔为 1 小时。 可用值：1h、12h、1d、2d、3d、15d、1w、1m、2m、3m、6m 默认值：1h	72 小时以上。此样本的计算持续时间以 ISO-8601 标准格式表示。

指标 **API** 的输出示例

例如， `/datacenter/cluster/nodes/{key}/metrics` API 检索节点的以下详细信息（以及其他信息）：

汇总值中的 95 百分位数表示，在此期间收集的样本中有 95% 的计数器值小于指定为 95 百分位数的值。

```
{
     "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
        }
      },
```

分析 **API** 的输出示例

例如， `/datacenter/cluster/nodes/analytics` API 检索所有节点的以下值（包括其他值）：

```
{     "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"
        }
      }
    },
```

可用 **API** 列表

下表详细介绍了 `/metrics`和 `/analytics` API。

这些 API 返回的 IOPS 和性能指标是双精度值，例如 `100.53`。不支持通过管道（|）和通配符（*）字符过滤这些浮点值。

HTTP 动词	路径	问题描述
GET	`/datacenter/cluster/clusters/{key}/metrics`	检索由集群键的输入参数指定的集群的性能数据（样本和摘要）。将返回集群键和 UUID 、时间范围、IOPS 、吞吐量和样本数等信息。
GET	`/datacenter/cluster/clusters/analytics`	检索数据中心中所有集群的高级性能指标。您可以根据所需条件筛选结果。将返回值，例如聚合 IOPS、吞吐量和收集周期（以小时为单位）。
GET	`/datacenter/cluster/nodes/{key}/metrics`	检索由节点键的输入参数指定的节点的性能数据（样本和摘要）。将返回节点 UUID、时间范围、IOPS、吞吐量、延迟和性能的摘要、收集的样本数量以及利用率百分比等信息。
GET	`/datacenter/cluster/nodes/analytics`	检索数据中心中所有节点的高级性能指标。您可以根据所需条件筛选结果。将返回节点和集群键等信息，以及聚合 IOPS、吞吐量和收集周期（以小时为单位）等值。
GET	`/datacenter/storage/aggregates/{key}/metrics`	检索由聚合键的输入参数指定的聚合的性能数据（样本和摘要）。将返回时间范围、IOPS 摘要、延迟、吞吐量和性能容量、为每个计数器收集的样本数以及利用率百分比等信息。
GET	`/datacenter/storage/aggregates/analytics`	检索数据中心中所有聚合的高级性能指标。您可以根据所需条件筛选结果。将返回聚合和集群键等信息，以及聚合 IOPS、吞吐量和收集周期（以小时为单位）等值。

HTTP 动词	路径	问题描述
GET	/datacenter/storage/luns/{key}/metrics /datacenter/storage/volumes/{key}/metrics	检索由 LUN 或卷键的输入参数指定的 LUN 或文件共享（卷）的性能数据（样本和摘要）。将返回相关信息，例如读取、写入和总 IOPS、延迟和吞吐量的最小值、最大值和平均值的摘要，以及为每个计数器收集的样本数。
GET	/datacenter/storage/luns/analytics /datacenter/storage/volumes/analytics	检索数据中心中所有 LUN 或卷的高级性能指标。您可以根据所需条件筛选结果。将返回存储 VM 和集群密钥等信息，以及聚合 IOPS、吞吐量和收集周期（以小时为单位）等值。
GET	/datacenter/svm/svms/{key}/metrics	检索由 storage VM 密钥的输入参数指定的 storage VM 的性能数据（示例和摘要）。将返回基于每个受支持协议的 IOPS 摘要，例如 `nvmf`，`fcp`，`iscsi`,`和 `nfs`、吞吐量、延迟以及收集的样本数。
GET	/datacenter/svm/svms/analytics	检索数据中心中所有存储 VM 的高级性能指标。您可以根据所需条件筛选结果。将返回存储 VM UUID、聚合 IOPS、延迟、吞吐量和收集周期（以小时为单位）等信息。
GET	/datacenter/network/ethernet/ports/{key}/metrics	检索由端口键的输入参数指定的特定以太网端口的性能指标。当从支持的范围提供间隔（时间范围）时，API 将返回累计计数器，例如该时间段内的最小值、最大值和平均性能值。
GET	/datacenter/network/ethernet/ports/analytics	检索数据中心环境中所有以太网端口的高级性能指标。返回端口的集群和节点密钥以及 UUID 、吞吐量、收集周期和利用率百分比等信息。您可以按可用参数筛选结果，例如端口密钥、利用率百分比、集群和节点名称以及 UUID 等。
GET	/datacenter/network/fc/interfaces/{key}/metrics	检索由接口键的输入参数指定的特定网络 FC 接口的性能指标。当从支持的范围提供间隔（时间范围）时，API 将返回累计计数器，例如该时间段内的最小值、最大值和平均性能值。

HTTP 动词	路径	问题描述
GET	/datacenter/network/fc/interfaces/analytics	检索数据中心环境中所有以太网端口的高级性能指标。将返回相关信息，例如集群和 FC 接口键以及 UUID、吞吐量、IOPS、延迟和存储 VM。您可以按可用参数筛选结果，例如集群和 FC 接口名称和 UUID、存储 VM、吞吐量等。
GET	/datacenter/network/fc/ports/{key}/metrics	检索由端口键的输入参数指定的特定 FC 端口的性能指标。当从支持的范围提供间隔（时间范围）时，API 将返回累计计数器，例如该时间段内的最小值、最大值和平均性能值。
GET	/datacenter/network/fc/ports/analytics	检索数据中心环境中所有 FC 端口的高级性能指标。返回端口的集群和节点密钥以及 UUID、吞吐量、收集周期和利用率百分比等信息。您可以按可用参数筛选结果，例如端口密钥、利用率百分比、集群和节点名称以及 UUID 等。
GET	/datacenter/network/ip/interfaces/{key}/metrics	检索由接口键的输入参数指定的网络 IP 接口的性能指标。当从支持的范围提供间隔（时间范围）时，API 将返回信息，例如样本数、累计计数器、吞吐量以及接收和传输的数据包数。
GET	/datacenter/network/ip/interfaces/analytics	检索数据中心环境中所有网络 IP 接口的高级性能指标。将返回集群和 IP 接口密钥及 UUID、吞吐量、IOPS 和延迟等信息。您可以按可用参数筛选结果，例如集群和 IP 接口名称及 UUID、IOPS、延迟、吞吐量等。

使用 **Active IQ Unified Manager** 中的 **API** 查看作业和系统详细信息

您可以使用 `jobs`类别下的 `management-server` API 查看异步操作的执行详细信息。 `management-server`类别下的 `system` API 可用于查看 Active IQ Unified Manager 环境中的实例详细信息。

查看作业

在 Active IQ Unified Manager 中，添加和修改资源等操作是通过同步和异步 API 调用执行的。计划异步执行的调用可以由为此调用创建的作业对象进行跟踪。每个作业对象都有一个用于标识的唯一键。每个作业对象都会返回作业对象 URI，供您访问和跟踪作业进度。您可以使用此 API 检索每次执行的详细信息。

通过使用此 API，您可以查询数据中心的所有作业对象，包括历史数据。默认情况下，查询所有作业将返回通过 Web UI 和 API 接口触发的最后 20 个作业的详细信息。使用内置筛选器查看特定作业。您还可以使用 Job 键查

询特定作业的详细信息，并对资源运行下一组操作。

类别	HTTP 谓词	路径	问题描述
management-server	GET	`/management-server/jobs`	返回所有作业的作业详细信息。在未指定任何排序顺序的情况下，最后提交的作业对象将返回在最上方。
management-server	GET	`/management-server/jobs/{key}` 输入 Job 对象的作业键以查看该作业的具体详细信息。	返回特定作业对象的详细信息。

查看系统详细信息

通过使用 `/management-server/system` API，您可以查询 Unified Manager 环境的实例特定详细信息。API 返回有关产品和服务的信息，例如系统上安装的 Unified Manager 版本、UUID、供应商名称、主机操作系统以及在 Unified Manager 实例上运行的服务的名称、描述和状态。

类别	HTTP 谓词	路径	问题描述
management-server	GET	`/management-server/system`	运行此 API 不需要输入参数。默认情况下，将返回当前 Unified Manager 实例的系统详细信息。

使用 Active IQ Unified Manager 中的 API 管理事件和警报

`management-server` 类别下的 `events`、 `alerts` 和 `scripts` API 使您能够管理 Active IQ Unified Manager 环境中的事件、警报以及与警报关联的脚本。

查看和修改事件

Unified Manager 接收在 ONTAP 上为由 Unified Manager 监控和管理的集群生成的事件。通过使用这些 API，您可以查看为集群生成的事件，并解决和更新它们。

通过对 `GET` API 运行 `/management-server/events` 方法，您可以查询数据中心中的事件，包括历史数据。使用内置过滤器（例如名称、影响级别、影响区域、严重性、状态、资源名称和资源类型）来查看特定事件。资源类型和区域参数返回有关发生事件的存储对象的信息，影响区域返回有关引发事件的问题的信息，例如可用性、容量、配置、安全性、保护和性能。

通过运行此 API 的 PATCH 操作，您可以为事件启用解决工作流。您可以将事件分配给自己或其他用户，并确认收到该事件。在对资源执行步骤以解决触发事件的问题后，您可以使用此 API 将事件标记为已解决。

有关事件的详细信息，请参见 "了解 Active IQ 平台事件"。

类别	HTTP 谓词	路径	问题描述
management-server	GET	`/management-server/events` `/management-server/events/{key}`	当您运行 Get ALL 方法时，响应正文由数据中心中所有事件的事件详细信息组成。当您通过特定键检索事件详细信息时，您可以查看特定事件的详细信息，并对资源运行下一组操作。响应正文由该事件的详细信息组成。
management-server	PATCH	`management-server/events/{key}`	运行此 API 以分配事件或将状态更改为“已确认”或“已解决”。您还可以使用此方法将此事件分配给自己或其他用户。这是一个同步操作。

管理提醒

事件会自动且持续地生成。只有当事件满足特定筛选条件时，Unified Manager 才会生成警报。您可以选择应为其生成警报的事件。通过使用 `/management-server/alerts` API，您可以配置警报，以便在发生特定事件或特定严重程度类型的事件时自动发送通知。

有关警报的详细信息，请参见 "了解警报"。

类别	HTTP 谓词	路径	问题描述
management-server	GET	`/management-server/alerts` `/management-server/alerts/{key}`	通过使用 alert 键，查询环境中的所有现有警报或特定警报。您可以查看环境中生成的警报的相关信息，例如警报描述、操作、发送通知的电子邮件 ID、事件和严重性。
management-server	POST	`/management-server/alerts`	通过此方法，您可以为特定事件添加警报。您必须添加警报名称、适用该警报的物理或逻辑资源或事件、警报是否已启用，以及是否要发送 SNMP 陷阱。您可以添加要为其生成警报的其他详细信息，例如操作、通知电子邮件 ID、脚本详细信息（如果您要添加警报脚本）等。
management-server	PATCH 和 DELETE	`management-server/events/{key}`	您可以使用这些方法来修改和删除特定的警报。您可以修改不同的属性，例如描述、名称以及启用和禁用警报。当不再需要警报时，您可以将其删除。

在选择用于添加警报的资源时，请注意，选择集群作为资源不会自动选择该集群中的存储对象。例如，如果为所有集群的所有关键事件创建警报，则只会收到集群关键事件的警报。您不会收到有关节点、聚合等上的关键事件的警报。

管理脚本

通过使用 `/management-server/scripts` API，您还可以将警报与触发警报时执行的脚本相关联。您可以使用脚本自动修改或更新 Unified Manager 中的多个存储对象。该脚本与警报相关联。当事件触发警报时，将执行脚本。您可以在生成警报时上传自定义脚本并测试其执行情况。您可以将警报与脚本关联，以便在 Unified Manager 中引发事件警报时执行脚本。

有关脚本的详细信息，请参见 "管理脚本"。

类别	**HTTP** 谓词	路径	问题描述
management-server	GET	`/management-server/scripts`	使用此 API 查询环境中的所有现有脚本。使用标准筛选和排序操作仅查看特定脚本。
management-server	POST	`/management-server/scripts`	使用此 API 可添加脚本的描述，并上传与警报关联的脚本文件。

管理工作负载

使用 **Active IQ Unified Manager** 中的 **API** 查看存储工作负载

此处列出的 API 使您能够查看数据中心中所有 ONTAP 集群的存储工作负载的合并列表。这些 API 还提供了 Active IQ Unified Manager 环境中配置的存储工作负载数量及其容量和性能（IOPS）统计信息的摘要视图。

查看存储工作负载

您可以使用以下方法查看数据中心所有集群中的所有存储工作负载。有关根据特定列筛选响应的信息，请参阅 Unified Manager 实例中提供的 API 参考文档。

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/workloads`

查看存储工作负载摘要

您可以使用以下方法评估已用容量、可用容量、已用 IOPS、可用 IOPS 以及每个性能服务级别管理的存储工作负载数。显示的存储工作负载可用于任何 LUN、NFS 文件共享或 CIFS 共享。此 API 提供存储工作负载概述、由 Unified Manager 调配的存储工作负载概述、数据中心概述，以及根据分配的性能服务级别提供的数据中心总空间、已用空间、可用空间和 IOPS 概述。响应此 API 收到的信息用于填充 Unified Manager UI 中的仪表板。

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/workloads-summary`

使用 **Active IQ Unified Manager** 中的 **API** 管理访问端点

您需要创建访问端点或逻辑接口 (LIF)，这是配置 Storage Virtual Machine (SVM)、LUN 和文件共享所必需的。您可以在 Active IQ Unified Manager 环境中查看、创建、修改和删除 SVM、LUN 或文件共享的访问端点。

查看访问端点

您可以使用以下方法查看 Unified Manager 环境中的访问端点列表。要查询特定 SVM、LUN 或文件共享的访问端点列表，需要输入 SVM、LUN 或文件共享的唯一标识符。您还可以输入唯一访问端点密钥以检索特定访问端点的详细信息。

类别	**HTTP** 谓词	路径

storage-provider	GET	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

添加访问端点

您可以创建自定义访问端点并为其分配所需的属性。您必须输入要创建的访问端点的详细信息作为输入参数。您可以使用此 API，或者 System Manager 或 ONTAP CLI 在每个节点上创建访问端点。创建访问端点支持 IPv4 和 IPv6 地址。

> 您必须为 SVM 配置每个节点最小数量的访问端点，才能成功配置 LUN 和文件共享。您应该为 SVM 在每个节点上配置至少两个访问端点，一个支持 CIFS 和/或 NFS 协议，另一个支持 iSCSI 或 FCP 协议。

类别	**HTTP** 谓词	路径
storage-provider	POST	`/storage-provider/access-endpoints`

删除访问端点

可以使用以下方法删除特定的访问端点。需要提供访问端点密钥作为输入参数来删除特定访问端点。

类别	**HTTP** 谓词	路径
storage-provider	DELETE	`/storage-provider/access-endpoints/{key}`

修改访问端点

您可以使用以下方法修改访问端点并更新其属性。您需要提供访问端点密钥才能修改特定访问端点。您还需要输入要更新的属性及其值。

类别	**HTTP** 谓词	路径
storage-provider	PATCH	`/storage-provider/access-endpoints/{key}`

在 **Active IQ Unified Manager** 中使用 **API** 管理 **Active Directory** 映射

您可以使用此处列出的 API 来管理 SVM 上的 Active Directory 映射，这是在 SVM 上调配 CIFS 共享所必需的。需要配置 Active Directory 映射，以便将 SVM 与 ONTAP 进行映射。

查看 **Active Directory** 映射

您可以通过以下方法查看 SVM Active Directory 映射的配置详细信息。要在 SVM 上查看 Active Directory 映射，需要输入 SVM 密钥。要查询特定映射的详细信息，必须输入映射密钥。

类别	**HTTP** 谓词	路径

storage-provider	GET	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

添加 **Active Directory** 映射

您可以使用以下方法在 SVM 上创建 Active Directory 映射。您必须输入映射详细信息作为输入参数。

类别	**HTTP** 谓词	路径
storage-provider	POST	`/storage-provider/active-directories-mappings`

使用 **Active IQ Unified Manager** 中的 **API** 管理文件共享

您可以使用 `/storage-provider/file-shares` API 查看、添加、修改和删除数据中心环境中的 CIFS 和 NFS 文件共享卷。

在配置文件共享卷之前，请确保已使用支持的协议创建和配置 SVM。如果在配置时分配性能服务级别（PSL）或存储效率策略（SEP），则应在创建文件共享之前创建 PSL 或 SEP。

查看文件共享

您可以使用以下方法查看 Unified Manager 环境中可用的文件共享卷。当您在 Active IQ Unified Manager 上将 ONTAP 集群添加为数据源时，这些集群的存储工作负载将自动添加到您的 Unified Manager 实例中。此 API 检索自动和手动添加到 Unified Manager 实例的文件共享。您可以通过使用文件共享密钥运行此 API 来查看特定文件共享的详细信息。

类别	HTTP 谓词	路径

storage-provider	GET	`/storage-provider/file-shares`
		
		`/storage-provider/file-shares/{key}`

添加文件共享

您可以使用以下方法在 SVM 中添加 CIFS 和 NFS 文件共享。必须输入要创建的文件共享的详细信息作为输入参数。您不能使用此 API 添加 FlexGroup 卷。

类别	HTTP 谓词	路径
storage-provider	POST	`/storage-provider/file-shares`

根据是否提供访问控制列表（ACL）参数或导出策略参数，将创建 CIFS 共享或 NFS 文件共享。如果不提供 ACL 参数的值，则不会创建 CIFS 共享，并且默认情况下会创建 NFS 共享，从而提供对所有人的访问权限。

创建数据保护卷：将文件共享添加到 SVM 时，默认装载的卷类型为 `rw`（读写）。要创建数据保护（DP）卷，请将 `dp`指定为 `type`参数的值。

删除文件共享

您可以使用以下方法删除特定文件共享。您需要输入文件共享密钥作为输入参数来删除特定的文件共享。

类别	HTTP 谓词	路径
storage-provider	DELETE	`/storage-provider/file-shares/{key}`

修改文件共享

可以使用以下方法修改文件共享并更新其属性。

需要提供文件共享密钥才能修改特定的文件共享。此外，需要输入要更新的属性及其值。

请注意，一次调用此 API 时只能更新一个属性。对于多个更新，需要多次运行此 API。

类别	HTTP 谓词	路径
storage-provider	PATCH	`/storage-provider/file-shares/{key}`

使用 **Active IQ Unified Manager** 中的 **API** 管理 **LUN**

您可以使用 `/storage-provider/luns` API 查看、添加、修改和删除数据中心环境中的 LUN。

在配置 LUN 之前，请确保已使用支持的协议创建和配置 SVM。如果在配置时分配性能服务级别（PSL）或存储效率策略（SEP），则应在创建 LUN 之前创建 PSL 或 SEP。

查看 LUN

您可以使用以下方法查看 Unified Manager 环境中的 LUN。当您将 ONTAP 集群作为数据源添加到 Active IQ Unified Manager 时，这些集群的存储工作负载将自动添加到您的 Unified Manager 实例中。此 API 检索自动和手动添加到 Unified Manager 实例的所有 LUN。您可以通过使用 LUN 密钥运行此 API 来查看特定 LUN 的详细信息。

类别	HTTP 谓词	路径

storage-provider	GET	`/storage-provider/luns`
		
		`/storage-provider/luns/{key}`

添加 LUN

您可以使用以下方法将 LUN 添加到 SVM。

类别	HTTP 谓词	路径
storage-provider	POST	`/storage-provider/luns`

在 cURL 请求中，如果您为输入中的可选参数 volume_name_tag 提供了值，则在 LUN 创建期间命名卷时将使用该值。此标记可方便地搜索卷。如果您在请求中提供了卷密钥，则会跳过标记。

删除 LUN

可以使用以下方法删除特定 LUN。必须提供 LUN 密钥才能删除特定 LUN。

如果您在 ONTAP 中创建了卷，然后通过 Unified Manager 在该卷上调配了 LUN，则当您使用此 API 删除所有 LUN 时，该卷也将从 ONTAP 集群中删除。

类别	HTTP 谓词	路径
storage-provider	DELETE	`/storage-provider/luns/{key}`

修改 LUN

可以使用以下方法修改 LUN 并更新其属性。需要提供 LUN 密钥才能修改特定 LUN。还需要输入要更新的 LUN 属性及其值。要使用此 API 更新 LUN 阵列，应查看 “使用 API 的建议” 中的建议。

一次调用此 API 只能更新一个属性。对于多次更新，您需要多次运行此 API。

类别	HTTP 谓词	路径
storage-provider	PATCH	`/storage-provider/luns/{key}`

在 **Active IQ Unified Manager** 中使用 **API** 管理性能服务级别

您可以通过使用 Active IQ Unified Manager 上的存储提供程序 API 来查看、创建、修改和删除性能服务级别。

查看性能服务级别

可以使用以下方法查看性能服务级别，以便将其分配给存储工作负载。API 列出所有系统定义和用户创建的性能服务级别，并检索所有性能服务级别的属性。如果要查询特定的性能服务级别，则需要输入性能服务级别的唯一 ID 以检索其详细信息。

类别	**HTTP** 谓词	路径

storage-provider	GET	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

添加性能服务级别

如果系统定义的性能服务级别未满足存储工作负载所需的服务级别目标（SLO），则可以使用以下方法创建自定义性能服务级别并将其分配给存储工作负载。输入要创建的性能服务级别的详细信息。对于 IOPS 属性，请确保输入有效的值范围。

类别	**HTTP** 谓词	路径
storage-provider	POST	`/storage-provider/performance-service-levels`

删除性能服务级别

您可以使用以下方法删除特定的 Performance Service Level。如果某个 Performance Service Level 已分配给工作负载，或者它是唯一可用的 Performance Service Level，则无法将其删除。您需要提供 Performance Service Level 的唯一 ID 作为输入参数，以删除特定的 Performance Service Level。

类别	**HTTP** 谓词	路径
storage-provider	DELETE	`/storage-provider/performance-service-levels/{key}`

修改性能服务级别

可以使用以下方法修改性能服务级别并更新其属性。无法修改系统定义或分配给工作负载的性能服务级别。需要提供唯一 ID 才能修改特定性能服务级别。还必须输入要更新的 IOPS 属性以及有效值。

类别	HTTP 谓词	路径
storage-provider	PATCH	`/storage-provider/performance-service-levels/{key}`

根据性能服务级别查看聚合功能

可以使用以下方法根据性能服务级别查询聚合功能。此 API 返回数据中心中可用的聚合列表，并指示这些聚合中可以支持的性能服务级别方面的功能。在卷上调配工作负载时，可以查看聚合支持特定性能服务级别的功能，并根据该功能调配工作负载。只有在使用 API 调配工作负载时，才能指定聚合。此功能在 Unified Manager Web UI 上不可用。

类别	HTTP 谓词	路径

storage-provider	GET	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

使用 **Active IQ Unified Manager** 中的 **API** 管理存储效率策略

您可以使用存储提供程序 API 查看、创建、修改和删除存储效率策略。

请注意以下几点：

- 在 Unified Manager 上创建工作负载时，不强制要求分配存储效率策略。
- 已向工作负载分配存储效率策略后，无法从该工作负载取消分配该策略。
- 如果工作负载在 ONTAP 卷上指定了一些存储设置，例如重复数据删除和数据压缩，则可以通过在 Unified Manager 上添加存储工作负载时应用的存储效率策略中指定的设置来覆盖这些设置。

查看存储效率策略

在将存储效率策略分配给存储工作负载之前，可以使用以下方法查看这些策略。此 API 列出所有系统定义和用户创建的存储效率策略，并检索所有存储效率策略的属性。如果要查询特定存储效率策略，则需要输入策略的唯一 ID 以检索其详细信息。

类别	HTTP 谓词	路径

storage-provider	GET	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

添加存储效率策略

您可以使用以下方法创建自定义存储效率策略，并在系统定义的策略不满足存储工作负载的配置要求时将其分配给存储工作负载。请输入要创建的存储效率策略的详细信息作为输入参数。

类别	**HTTP** 谓词	路径
storage-provider	POST	`/storage-provider/storage-efficiency-policies`

删除存储效率策略

您可以使用以下方法删除特定的存储效率策略。如果存储效率策略已分配给工作负载，或者它是唯一可用的存储效率策略，则无法删除该策略。您需要提供存储效率策略的唯一 ID 作为输入参数，以删除特定的存储效率策略。

类别	**HTTP** 谓词	路径
storage-provider	DELETE	`/storage-provider/storage-efficiency-policies/{key}`

修改存储效率策略

可以使用以下方法修改存储效率策略并更新其属性。无法修改系统定义或分配给工作负载的存储效率策略。需要提供存储效率策略的唯一 ID 才能修改特定的存储效率策略。此外，需要提供要更新的属性及其值。

类别	**HTTP** 谓词	路径
storage-provider	PATCH	`/storage-provider/storage-efficiency-policies/{key}`

存储管理的常见工作流程

了解 **Active IQ Unified Manager** 中用于存储管理的常见 **API** 工作流

常见工作流为客户端应用程序开发人员提供了客户端应用程序如何调用 Active IQ Unified Manager API 以执行常见存储管理功能的示例。本节包含其中一些示例工作流。

工作流描述了一些常用的存储管理用例以及供您使用的示例代码。每个任务都使用由一个或多个 API 调用组成的工作流流程进行描述。

了解工作流程中使用的 **API** 调用

您可以从 Unified Manager 实例查看在线文档页面，其中包含每个 REST API 调用的详细信息。本文档不重复在线文档的详细信息。本文档中工作流示例中使用的每个 API 调用仅包含在文档页面上查找该调用所需的信息。找到特定 API 调用后，您可以查看该调用的完整详细信息，包括输入参数、输出格式、HTTP 状态代码和请求处理类型。

工作流程中每个 API 调用都包含以下信息，以帮助在文档页面上查找该调用：

- 类别：API 调用在文档页面上按功能相关的区域或类别进行组织。要查找特定的 API 调用，请滚动到页面底部，然后单击适用的 API 类别。

- HTTP 谓词（调用）：HTTP 谓词标识对资源执行的操作。每个 API 调用都通过单个 HTTP 谓词执行。
- 路径：路径确定在执行调用时应用操作的特定资源。路径字符串附加到核心 URL 以形成标识资源的完整 URL。

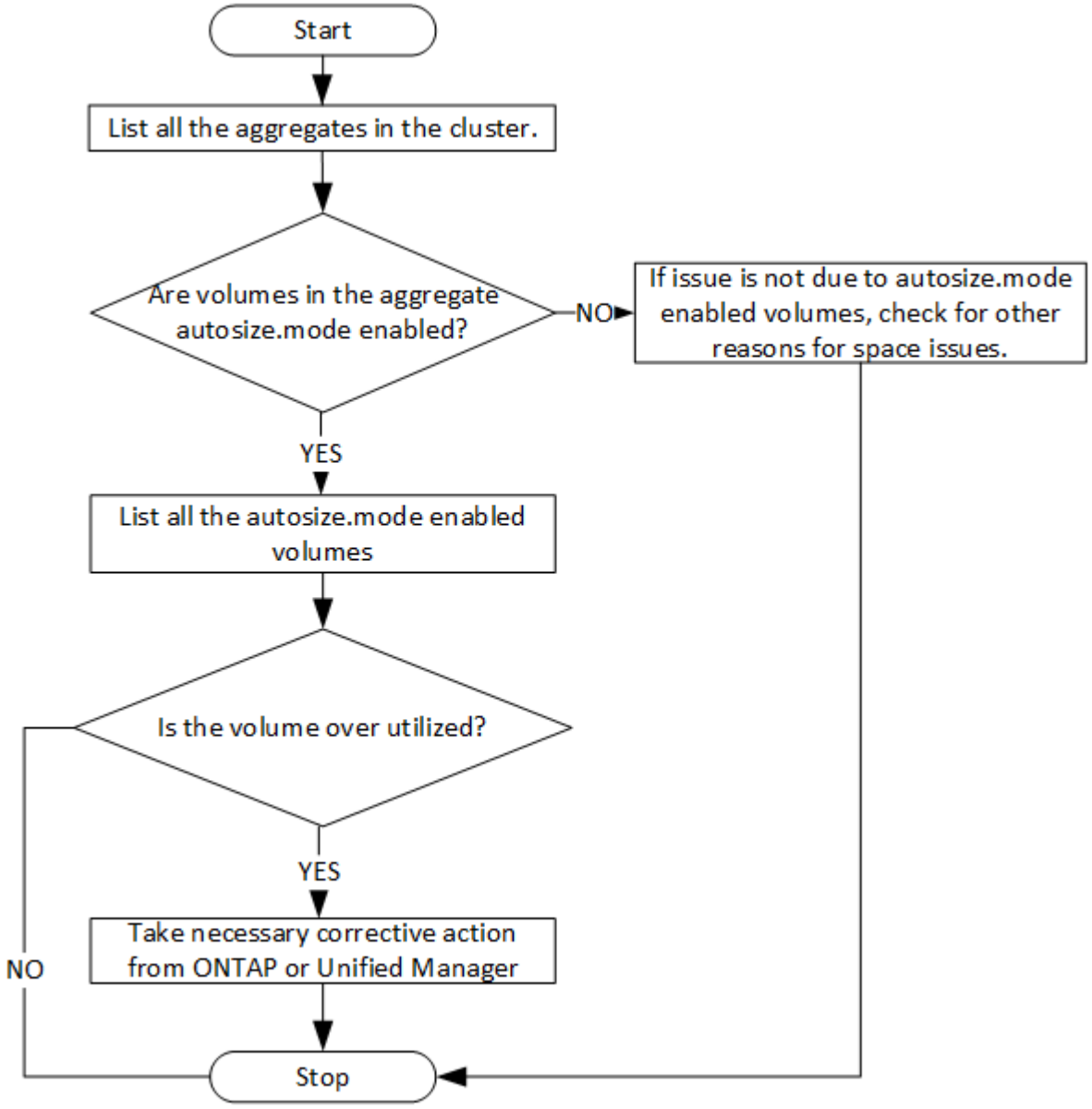
使用 **Active IQ Unified Manager API** 确定聚合中的空间问题

您可以使用 Active IQ Unified Manager 中的数据中心 API 来监控卷中空间的可用性和利用率。您可以确定卷中的空间问题，并识别过度使用或未充分使用的存储资源。

用于聚合的数据中心 API 检索有关可用和已用空间以及节省空间效率设置的相关信息。您还可以根据指定的属性筛选检索到的信息。

确定聚合中是否缺少空间的一种方法是验证环境中是否存在启用了 autosize-mode 的卷。然后，您应该识别哪些卷被过度使用，并执行任何纠正措施。

以下流程图说明了检索有关启用了 autosize-mode 的卷的信息的过程：



此流程假设集群已在 ONTAP 中创建并添加到 Unified Manager 中。

1. 获取集群密钥，除非您知道其值：

类别	**HTTP** 谓词	路径
数据中心	GET	`/datacenter/cluster/clusters`

2. 使用集群键作为筛选参数，查询该集群上的聚合。

类别	**HTTP** 谓词	路径
数据中心	GET	`/datacenter/storage/aggregates`

3. 从响应中，分析聚合的空间使用情况，并确定哪些聚合存在空间问题。对于每个存在空间问题的聚合，请从同一个 JSON 输出中获取聚合键。
4. 使用每个聚合键，筛选所有卷，其 autosize.mode 参数值为 `grow`.

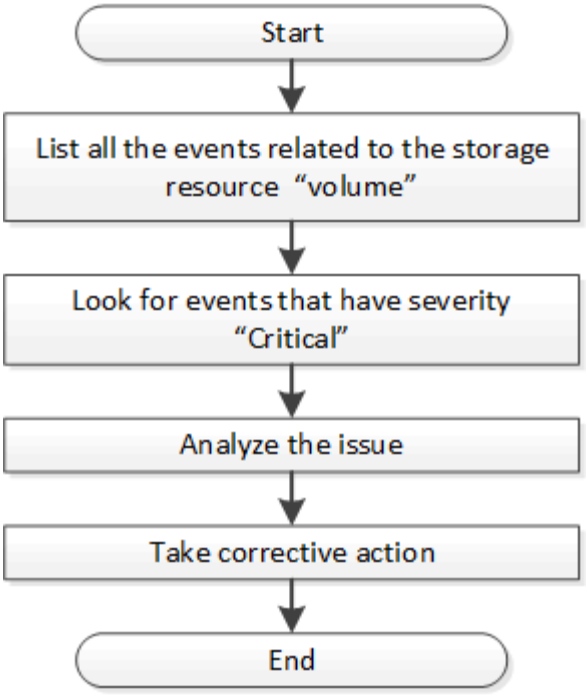
类别	**HTTP** 谓词	路径
数据中心	GET	`/datacenter/storage/volumes`

5. 分析哪些卷被过度使用。
6. 执行任何必要的纠正措施，例如跨聚合移动卷，以解决卷中的空间问题。您可以从 ONTAP 或 Unified Manager Web UI 执行这些操作。

使用 **Active IQ Unified Manager** 事件 **API** 确定存储对象问题

当数据中心中的存储对象超过阈值时，您会收到有关该事件的通知。使用此通知，您可以使用 `events` API 分析问题并采取纠正措施。

此工作流以卷作为资源对象为例。您可以使用 `events` API 检索与某个卷相关的事件列表，分析该卷的关键问题，然后采取纠正措施来解决该问题。



在采取补救措施之前，请按照下面的步骤确定卷中的问题。

步骤

1. 请分析数据中心卷的关键 Active IQ Unified Manager 事件通知。
2. 使用 /management-server/events API 中的以下参数查询卷的所有事件：
   "resource_type": "volume"
   "severity": "critical"

类别	**HTTP** 谓词	路径
management-server	GET	/management-server/events

3. 查看输出并分析特定卷中的问题。
4. 使用 Unified Manager REST API 或 Web UI 执行必要的操作以解决问题。

使用 **Active IQ Unified Manager** 网关 **API** 对 **ONTAP** 卷进行故障排除

网关 API 充当网关，用于调用 ONTAP API 来查询有关您的 ONTAP 存储对象的信息，并采取补救措施来解决所报告的问题。

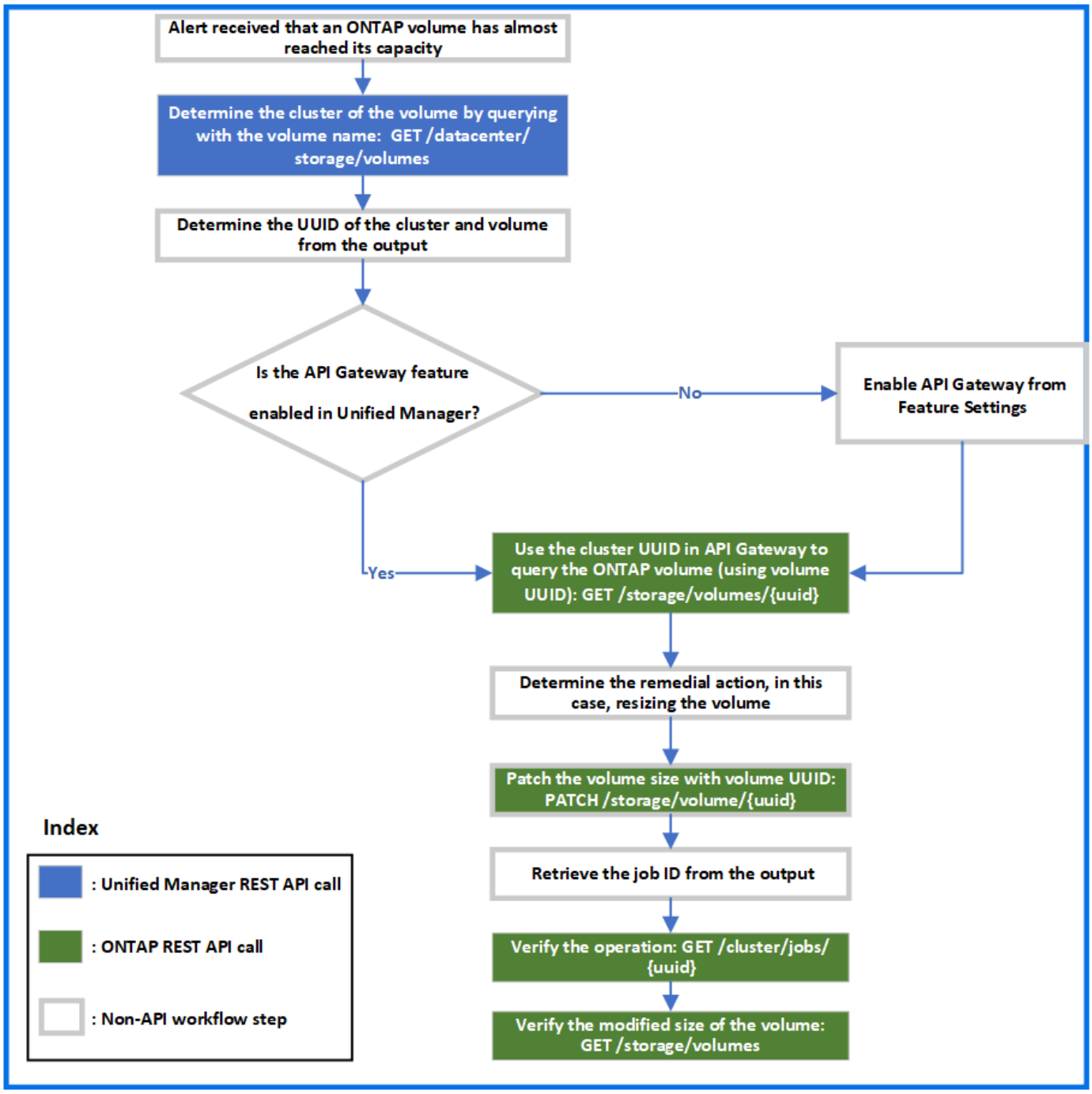
此工作流采用了一个示例用例，即当 ONTAP 卷几乎达到其容量时引发事件。该工作流还演示了如何通过结合调用 Active IQ Unified Manager 和 ONTAP REST API 来解决此问题。

在运行工作流程步骤之前，请确保执行以下操作：

- 您知道网关 API 及其使用方式。有关信息，请参见 "通过代理访问 ONTAP API"。
- 您了解 ONTAP REST API 的使用。有关使用 ONTAP REST API 的信息，请参见 "ONTAP Automation 文档"。
- 您是应用程序管理员。

- ONTAP 9.5 或更高版本支持要在其上运行 REST API 操作的集群，并且该集群已通过 HTTPS 添加到 Unified Manager。

下图说明了解决 ONTAP 卷容量使用问题的工作流程中的每个步骤。



工作流程涵盖了 Unified Manager 和 ONTAP REST API 的调用点。

1. 请注意通知卷容量利用率的事件中的卷名称。
2. 使用卷名作为 name 参数中的值，通过运行以下 Unified Manager API 查询卷。

类别	**HTTP** 谓词	路径
数据中心	GET	`/datacenter/storage/volumes`

3. 从输出中检索集群 UUID 和卷 UUID。
4. 在 Unified Manager Web UI 上，导航到 常规 > 功能设置 > **API** 网关 以验证是否已启用 API 网关功能。除非已启用，否则您无法调用网关类别下的 API。如果此功能已禁用，请将其启用。
5. 使用集群 UUID 通过 API 网关运行 ONTAP API `/storage/volumes/{uuid}`。当卷 UUID 作为 API 参数传递时，查询将返回卷详细信息。

   要通过 API 网关运行 ONTAP API，Unified Manager 凭据会在内部传递以进行身份验证，并且您无需为单个集群访问执行额外的身份验证步骤。

类别	**HTTP** 谓词	路径

Unified Manager：网关
 	
ONTAP：存储
	GET	网关 API：
		`/gateways/{uuid}/{path}`
		
		ONTAP API:
		`/storage/volumes/{uuid}`

> 在 /gateways/{uuid}/{path} 中，{uuid} 的值必须替换为要对其执行 REST 操作的集群 UUID 。{path} 必须替换为 ONTAP REST URL /storage/volumes/{uuid}。

附加的 URL 是： `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

运行 GET 操作时，生成的 URL 为：
`GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes/{volume_uuid}`

示例 **cURL** 命令

```
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. 从输出中确定大小、使用情况以及要采取的补救措施。在此工作流程中，采取的补救措施是调整卷大小。
7. 使用集群 UUID 并通过 API 网关运行以下 ONTAP API 以调整卷大小。有关网关和 ONTAP API 的输入参数的信息，请参阅步骤 5。

类别	HTTP 谓词	路径

Unified Manager：网关
 	
ONTAP：存储
	PATCH	网关 API：
		`/gateways/{uuid}/{path}`
		
		ONTAP API:
		`/storage/volumes/{uuid}`

除了集群 UUID 和卷 UUID 之外，您还必须为用于调整卷大小的 size 参数输入一个值。请确保输入的值_以字节为单位_。例如，如果要将卷的大小从 100 GB 增加到 120 GB，请在查询结尾处输入参数 size 的值： `-d {\"size\": 128849018880}"`

示例 **cURL** 命令

```
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}"
```

JSON 输出返回作业 UUID。

8. 使用作业 UUID 验证作业是否成功运行。使用集群 UUID 和作业 UUID 通过 API 网关运行以下 ONTAP API。有关网关和 ONTAP API 的输入参数的信息，请参见步骤 5。

类别	HTTP 谓词	路径

Unified Manager：网关
 	
ONTAP: 集群
	GET	网关 API：
		`/gateways/{uuid}/{path}`
		
		ONTAP API：
		`/cluster/jobs/{uuid}`

返回的 HTTP 代码与 ONTAP REST API HTTP 状态代码相同。

9. 运行以下 ONTAP API 以查询调整大小的卷的详细信息。有关网关和 ONTAP API 的输入参数的信息，请参阅步骤 5。

类别	HTTP 谓词	路径

Unified Manager：网关
 	
ONTAP：存储
	GET	网关 API：
		`/gateways/{uuid}/{path}`
		
		ONTAP API:
		`/storage/volumes/{uuid}`

输出显示增加的卷大小为 120 GB。

用于工作负载管理的工作流

在 **Active IQ Unified Manager** 中配置和修改存储工作负载

使用 Active IQ Unified Manager，您可以调配和修改存储工作负载（LUN、NFS 文件共享和 CIFS 共享）。调配包括多个步骤，从创建存储虚拟机（SVM）到对存储工作负载应用性能服务级别和存储效率策略。修改工作负载包括修改特定参数并在其上启用其他功能的步骤。

描述了以下工作流程：

- 用于在 Unified Manager 上配置 Storage Virtual Machines（SVM）的工作流。

  在 Unified Manager 上配置 LUN 或文件共享之前，需要执行此工作流。

- 配置文件共享。
- 配置 LUN。
- 修改 LUN 和文件共享（通过使用更新存储工作负载的性能服务级别参数的示例）。
- 修改 NFS 文件共享以支持 CIFS 协议
- 修改工作负载以将 QoS 升级为 AQoS

对于每个配置工作流（LUN 和文件共享），请确保您已完成验证集群上 SVM 的工作流。

在工作流程中使用每个 API 之前，您还必须阅读建议和限制。有关 API 的相关详细信息，请参阅相关概念和参考资料中列出的各个部分。

使用 **Active IQ Unified Manager API** 验证 **ONTAP** 集群上的 **SVM**

在调配文件共享或 LUN 之前，必须验证集群上是否创建了 Storage Virtual Machine（SVM）。

工作流假定 ONTAP 集群已添加到 Unified Manager 中，并且已获取集群密钥。集群应具有在其上调配 LUN 和文件共享所需的许可证。

1. 验证集群是否创建了 SVM。

类别	**HTTP** 谓词	路径
数据中心	GET	`/datacenter/svm/svms` `/datacenter/svm/svms/{key}`

示例 **cURL**

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept:
```

```
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. 如果未返回 SVM 密钥，则创建 SVM。要创建 SVM，您需要用于配置 SVM 的群集密钥。您还需要指定 SVM 名称。请按照以下步骤操作。

类别	**HTTP** 谓词	路径
数据中心	GET	`/datacenter/cluster/clusters` `/datacenter/cluster/clusters/{key}`

获取集群密钥。

示例 **cURL**

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

3. 从输出中获取 cluster 键，然后将其用作创建 SVM 的输入。

> 在创建 SVM 时，请确保它支持在其上调配 LUN 和文件共享所需的所有协议，例如 CIFS 、NFS、FCP 和 iSCSI。如果 SVM 不支持所需的服务，调配工作流可能会失败。建议在 SVM 上也启用相应类型工作负载的服务。

类别	**HTTP** 谓词	路径
数据中心	POST	`/datacenter/svm/svms`

示例 **cURL**

输入 SVM 对象详细信息作为输入参数。

```
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\"}"
```

JSON 输出将显示可用于验证您创建的 SVM 的作业对象键。

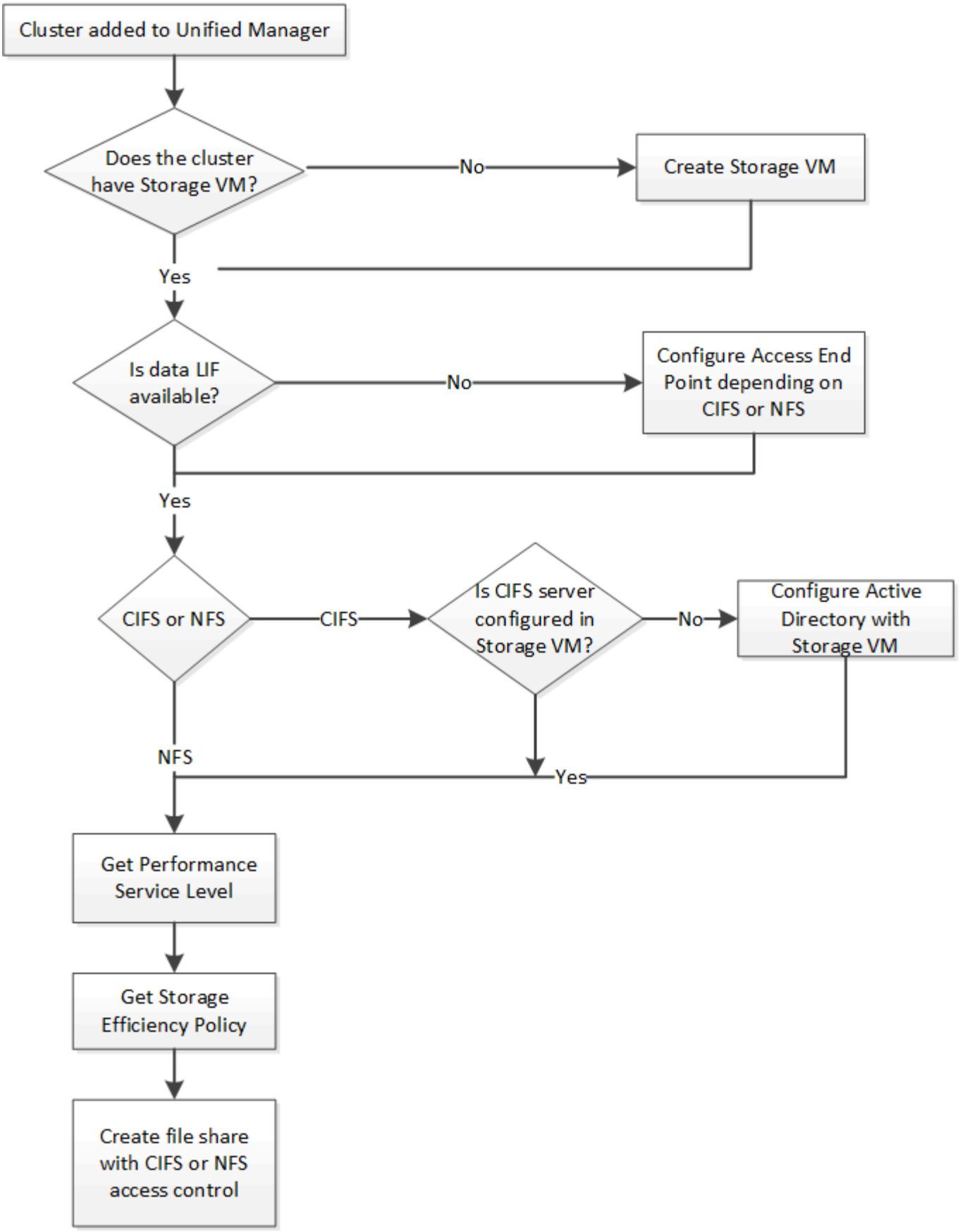
4. 使用作业对象键进行查询以验证 SVM 创建。如果 SVM 创建成功，则在响应中返回 SVM 键。

类别	**HTTP** 谓词	路径
management-server	GET	`/management-server/jobs/{key}`

使用 **Active IQ Unified Manager API** 设置 **CIFS** 和 **NFS** 文件共享

您可以使用作为 Active IQ Unified Manager 一部分提供的配置 API，在您的 Storage Virtual Machines (SVM) 上配置 CIFS 共享和 NFS 文件共享。此配置工作流详细介绍了在创建文件共享之前检索 SVM、性能服务级别和存储效率策略的密钥的步骤。

下图说明了文件共享调配工作流中的每个步骤。它包括调配 CIFS 共享和 NFS 文件共享。


Cluster added to Unified Manager
Does the cluster have Storage VM?
No
Create Storage VM
Yes
Is data LIF available?
No
Configure Access End Point depending on CIFS or NFS
Yes
CIFS or NFS
CIFS
Is CIFS server configured in Storage VM?
No
Configure Active Directory with Storage VM
NFS
Yes
Get Performance Service Level
Get Storage Efficiency Policy
Create file share with CIFS or NFS access control

确保以下内容：

- ONTAP 集群已添加到 Unified Manager 中，并且已获取集群密钥。
- 已在群集上创建了 SVM。
- SVM 支持 CIFS 和 NFS 服务。如果 SVM 不支持所需的服务，则配置文件共享可能会失败。
- FCP 端口已联机以进行端口配置。

1. 确定要在其上创建 CIFS 共享的 SVM 上是否有可用的数据 LIF 或访问端点。获取 SVM 上可用访问端点的列表：

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/access-endpoints` `/storage-provider/access-endpoints/{key}`

示例 **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. 如果您的访问端点在列表中可用，请获取访问端点密钥，否则创建访问端点。

请确保创建的访问端点已启用 CIFS 协议。除非您创建了已启用 CIFS 协议的访问端点，否则配置 CIFS 共享将失败。

类别	**HTTP** 谓词	路径
storage-provider	POST	`/storage-provider/access-endpoints`

示例 **cURL**

必须输入要创建的访问端点的详细信息作为输入参数。

```
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}"
```

JSON 输出显示一个作业对象键，可用于验证您创建的访问端点。

3. 验证访问端点：

类别	**HTTP** 谓词	路径
management-server	GET	`/management-server/jobs/{key}`

4. 确定是必须创建 CIFS 共享还是 NFS 文件共享。要创建 CIFS 共享，请按照以下子步骤操作：

   a. 确定是否在您的 SVM 上配置了 CIFS 服务器，即确定是否在 SVM 上创建了 Active Directory 映射。

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/active-directories-mappings`

   b. 如果创建了 Active Directory 映射，请获取密钥，否则在 SVM 上创建 Active Directory 映射。

类别	**HTTP** 谓词	路径
storage-provider	POST	`/storage-provider/active-directories-mappings`

   示例 **cURL**

   您必须输入用于创建 Active Directory 映射的详细信息，作为输入参数。

```
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\"}"
```

+
这是一个同步调用，您可以在输出中验证 Active Directory 映射的创建。如果发生错误，将显示错误消息，以便您排除故障并重新运行请求。

5. 获取要在其上创建 CIFS 共享或 NFS 文件共享的 SVM 的 SVM 密钥，如 *Verifying SVMs on clusters* 工作流主题中所述。
6. 通过运行以下 API 并从响应中检索密钥，获取性能服务级别的密钥。

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/performance-service-levels`

您可以通过将 `system_defined`输入参数设置为 `true`来检索系统定义的性能服务级别的详细信息。从输出中，获取要应用于文件共享的性能服务级别的键。

7. （可选）通过运行以下 API 并从响应中检索密钥，获取要应用于文件共享的存储效率策略的存储效率策略密钥。

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/storage-efficiency-policies`

8. 创建文件共享。您可以通过指定访问控制列表和导出策略来创建同时支持 CIFS 和 NFS 的文件共享。如果您希望创建仅支持卷上其中一种协议的文件共享，以下子步骤提供了相关信息。在创建 NFS 共享后，您还可以更新 NFS 文件共享以包含访问控制列表。有关信息，请参见_修改存储工作负载_主题。

   a. 如果仅创建 CIFS 共享，请收集有关访问控制列表（ACL）的信息。要创建 CIFS 共享，请为以下输入参数提供有效值。对于您分配的每个用户组，在调配 CIFS/SMB 共享时会创建 ACL。根据您为 ACL 和 Active Directory 映射输入的值，在创建 CIFS 共享时将确定访问控制和映射。

      带有示例值的 **cURL** 命令

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    },
```

b. 对于仅创建 NFS 文件共享，请收集与导出策略相关的信息。要创建 NFS 文件共享，请为以下输入参数提供有效值。根据您的值，导出策略在创建时与 NFS 文件共享相关联。

> 在配置 NFS 共享时，可以通过提供所有必需值来创建导出策略，也可以提供导出策略密钥并重用现有导出策略。如果要重用存储 VM 的导出策略，则需要添加导出策略密钥。除非您知道密钥，否则可以使用 `/datacenter/protocols/nfs/export-policies` API 检索导出策略密钥。要创建新策略，必须输入以下示例中显示的规则。对于输入的规则，API 尝试通过匹配主机、存储 VM 和规则来搜索现有导出策略。如果存在现有导出策略，则使用该策略。否则，将创建一个新的导出策略。

带有示例值的 **cURL** 命令

```
"export_policy": {
      "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
      "name_tag": "ExportPolicyNameTag",
      "rules": [
        {
          "clients": [
            {
              "match": "0.0.0.0/0"
            }
```

配置访问控制列表和导出策略后，为 CIFS 和 NFS 文件共享的强制输入参数提供有效值：

> 存储效率策略是用于创建文件共享的可选参数。

类别	**HTTP** 谓词	路径
storage-provider	POST	`/storage-provider/file-shares`

JSON 输出显示一个作业对象键，您可以使用它来验证您创建的文件共享。使用查询作业时返回的作业对象键来验证文件共享的创建：

类别	**HTTP** 谓词	路径
management-server	GET	`/management-server/jobs/{key}`

在响应末尾，您会看到创建的文件共享的密钥。

```
    ],
    "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. 通过使用返回的密钥运行以下 API 来验证文件共享的创建：

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/file-shares/{key}`

JSON 输出示例

可以看到， `/storage-provider/file-shares` 的 POST 方法在内部调用每个功能所需的所有 API 并创建对象。例如，它调用 `/storage-provider/performance-service-levels/` API 在文件共享上分配性能服务级别。

```
{
    "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": [
```

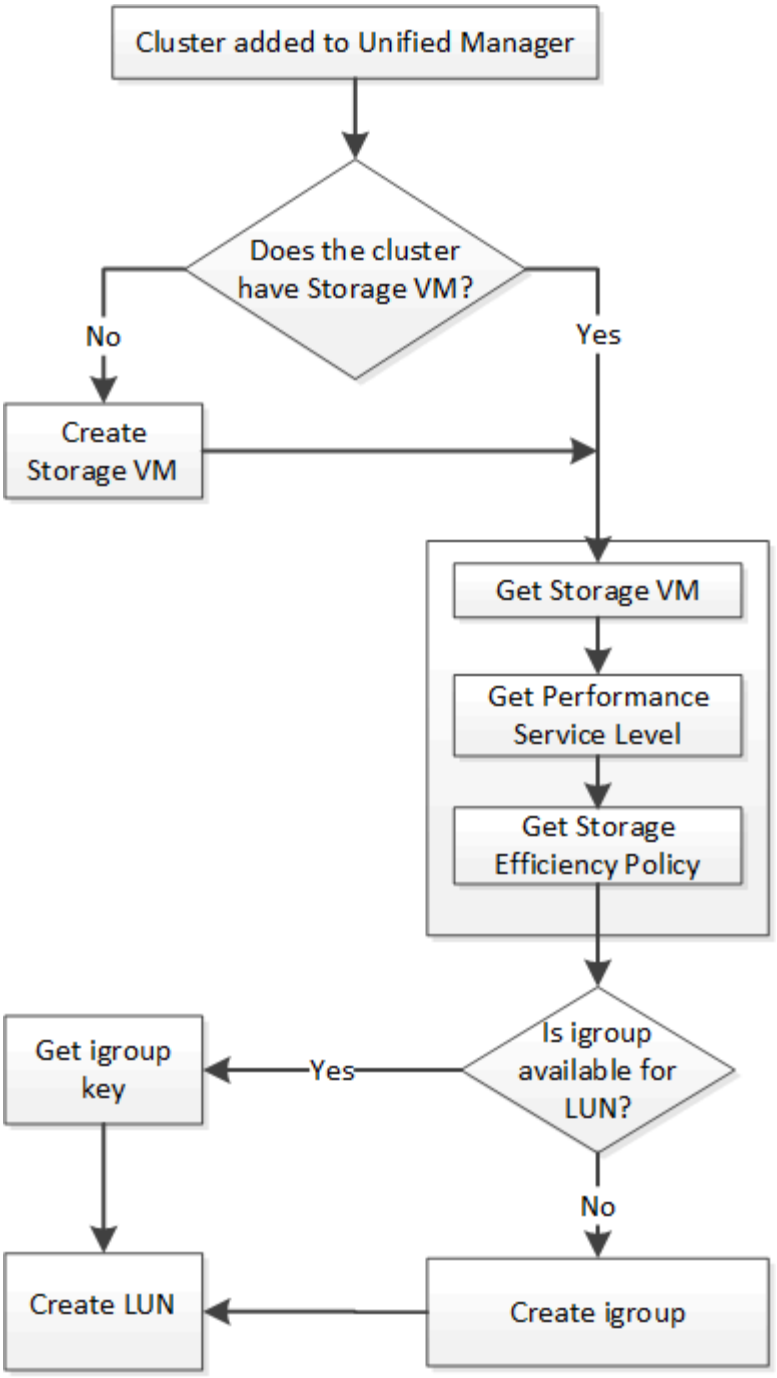
```
            {
                "anonymous_user": "65534",
                "clients": [
                    {
                        "match": "0.0.0.0/0"
                    }
                ],
                "index": 1,
                "protocols": [
                    "nfs3",
                    "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"
        }
    }
}
```

使用 **Active IQ Unified Manager API** 配置 **LUN**

您可以使用作为 Active IQ Unified Manager 一部分提供的资源调配 API 在 Storage Virtual Machine (SVM) 上配置 LUN。此资源调配工作流详细介绍了在创建 LUN 之前检索 SVM、性能服务级别和存储效率策略的密钥的步骤。

下图说明了 LUN 配置工作流中的步骤。



此工作流假定 ONTAP 集群已添加到 Unified Manager 中，并且已获取集群密钥。此工作流还假定已在集群上创建了 SVM。

1. 获取要在其上创建 LUN 的 SVM 的 SVM 密钥，如 *Verifying SVMs on clusters* 工作流主题中所述。
2. 通过运行以下 API 并从响应中检索密钥，获取性能服务级别的密钥。

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/performance-service-levels`

您可以通过将 `system_defined`输入参数设置为 `true`来检索系统定义的性能服务级别的详细信息。从输出中，获取要在 LUN 上应用的性能服务级别的键。

3. （可选）通过运行以下 API 并从响应中检索密钥，获取要应用于 LUN 的存储效率策略的存储效率策略密钥。

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/storage-efficiency-policies`

4. 确定是否已创建启动器组（igroup）以授予对要创建的 LUN 目标的访问权限。

类别	**HTTP** 谓词	路径
数据中心	GET	`/datacenter/protocols/san/igroups` `/datacenter/protocols/san/igroups/{key}`

您必须输入用于指示 igroup 具有授权访问权限的 SVM 的参数值。此外，如果要查询特定的 igroup，请输入 igroup 名称（键）作为输入参数。

5. 在输出中，如果可以找到要授予访问权限的 igroup，请获取密钥。否则，请创建 igroup。

类别	**HTTP** 谓词	路径
数据中心	POST	`/datacenter/protocols/san/igroups`

必须输入要创建的 igroup 的详细信息作为输入参数。这是一个同步调用，您可以在输出中验证创建的 igroup。如果发生错误，将显示一条消息，供您进行故障排除并重新运行 API。

6. 创建 LUN。

类别	**HTTP** 谓词	路径
storage-provider	POST	`/storage-provider/luns`

要创建 LUN，请确保已将检索到的值添加为必需输入参数。

存储效率策略是用于创建 LUN 的可选参数。

示例 **cURL**

您必须输入要创建的 LUN 的所有详细信息作为输入参数。

JSON 输出将显示可用于验证您创建的 LUN 的作业对象键。

7. 使用在查询作业时返回的作业对象键来验证 LUN 创建：

类别	**HTTP** 谓词	路径
management-server	GET	`/management-server/jobs/{key}`

在响应的末尾，您将看到创建的 LUN 的键。

8. 使用返回的密钥运行以下 API，以验证 LUN 的创建：

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/luns/{key}`

JSON 输出示例

可以看到， `/storage-provider/luns` 的 POST 方法在内部调用每个函数所需的所有 API 并创建对象。例如，它调用用于在 LUN 上分配性能服务级别的 `/storage-provider/performance-service-levels/` API。

== LUN 创建或映射失败的故障排除步骤

完成此工作流后，您可能仍会看到 LUN 创建失败。即使成功创建了 LUN，由于在创建 LUN 的节点上 SAN LIF 或访问端点不可用，与 igroup 的 LUN 映射也可能会失败。如果发生故障，您可以看到以下消息：

```
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.
```

按照这些疑难解答步骤来解决此失败问题。

1. 在尝试创建 LUN 的 SVM 上创建支持 ISCSI/FCP 协议的访问端点。

类别	**HTTP** 谓词	路径
storage-provider	POST	`/storage-provider/access-endpoints`

示例 **cURL**

必须输入要创建的访问端点的详细信息作为输入参数。

> 确保在输入参数中添加了用于指示 LUN 主节点的地址和用于指示主节点配对节点的 ha_address。运行此操作时，它会在主节点和配对节点上创建访问端点。

2. 使用 JSON 输出中返回的作业对象键查询作业，以验证其已成功运行并在 SVM 上添加了访问端点，并且已在 SVM 上启用了 iSCSI/FCP 服务。

类别	**HTTP** 谓词	路径
management-server	GET	`/management-server/jobs/{key}`

JSON 输出示例

在输出结束时，您可以看到创建的访问端点的密钥。在下面的输出中，"name": "accessEndpointKey" 值表示在 LUN 的主节点上创建的访问端点，其密钥为 9c964258-14ef-11ea-95e2-00a098e32c28。"name": "accessEndpointHAKey" 值表示在主节点的配对节点上创建的访问端点，其密钥为 9d347006-14ef-11ea-8760-00a098e3215f。

3. 修改 LUN 以更新 igroup 映射。有关工作流修改的详细信息，请参见 “修改存储工作负载”。

类别	**HTTP** 谓词	路径
storage-provider	PATCH	`/storage-provider/lun/{key}`

在输入中，指定要用于更新 LUN 映射的 igroup 密钥，以及 LUN 密钥。

示例 **cURL**

JSON 输出将显示一个作业对象键，可用于验证映射是否成功。

4. 通过使用 LUN 密钥进行查询来验证 LUN 映射。

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/luns/{key}`

JSON 输出示例

在输出中，您可以看到 LUN 已成功映射到最初为其配置的 igroup（键 d19ec2fa-fec7-11e8-b23d-00a098e32c28）。

修改存储工作负载

使用 **Active IQ Unified Manager** 中的 **API** 修改存储工作负载

修改存储工作负载包括更新缺少参数的 LUN 或文件共享，或更改现有参数。

此工作流以更新 LUN 和文件共享的性能服务级别为例。

工作流假定 LUN 或文件共享已使用性能服务级别进行调配。

修改文件共享

修改文件共享时，可以更新以下参数：

- 容量或大小。
- 在线或离线设置。
- 存储效率策略。
- 性能服务级别。
- 访问控制列表（ACL）设置。
- 导出策略设置。您还可以删除导出策略参数并还原文件共享上的默认（空）导出策略规则。

在单个 API 运行期间，您只能更新一个参数。

此过程描述向文件共享添加性能服务级别。您可以使用相同的过程来更新任何其他文件共享属性。

1. 获取要更新的文件共享的 CIFS 共享或 NFS 文件共享密钥。此 API 查询数据中心上的所有文件共享。如果您已经知道文件共享密钥，请跳过此步骤。

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/file-shares`

2. 使用获取的文件共享密钥运行以下 API，查看文件共享的详细信息。

类别	**HTTP** 谓词	路径
storage-provider	GET	`/storage-provider/file-shares/{key}`

在输出中查看文件共享的详细信息。

```
"assigned_performance_service_level": {
        "key": null,
        "name": "Unassigned",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
      },
```

3. 获取要在此文件共享上分配的性能服务级别的密钥。当前未为其分配任何策略。

类别	**HTTP** 谓词	路径
性能服务级别	GET	`/storage-provider/performance-service-levels`

您可以通过将 `system_defined`输入参数设置为 `true`来检索系统定义的性能服务级别的详细信息。从输出中，获取要应用于文件共享的性能服务级别的键。

4. 对文件共享应用性能服务级别。

类别	HTTP 谓词	路径
存储提供商	PATCH	`/storage-provider/file-shares/{key}`

在输入中，必须仅指定要更新的参数以及文件共享键。在本例中，它是性能服务级别的键。

示例 **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\" },
}"
```

JSON 输出显示一个作业对象，您可以使用该对象来验证归属节点和配对节点上的访问端点是否已成功创建。

5. 使用输出中显示的作业对象键，验证是否已将性能服务级别添加到文件共享。

类别	HTTP 谓词	路径
管理服务器	GET	`/management-server/jobs/{key}`

如果按作业对象的 ID 查询，您会看到文件共享是否成功更新。如果发生故障，请排除故障并再次运行 API。成功创建后，查询文件共享以查看修改的对象：

类别	HTTP 谓词	路径
storage-provider	GET	`/storage-provider/file-shares/{key}`

在输出中查看文件共享的详细信息。

```
"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"
```

```
            }
        }
```

更新 LUN

更新 LUN 时，可以修改以下参数：

- 容量或大小
- 在线或离线设置
- 存储效率策略
- 性能服务级别
- LUN 映射

> 在单个 API 运行期间，您只能更新一个参数。

此过程描述向 LUN 添加性能服务级别。您可以使用相同的过程来更新任何其他 LUN 属性。

1. 获取要更新的 LUN 的 LUN 密钥。此 API 返回数据中心中所有 LUN 的详细信息。如果您已经知道 LUN 密钥，请跳过此步骤。

类别	HTTP 谓词	路径
存储提供商	GET	`/storage-provider/luns`

2. 使用您获取的 LUN 密钥运行以下 API ，以查看 LUN 的详细信息。

类别	HTTP 谓词	路径
存储提供商	GET	`/storage-provider/luns/{key}`

   在输出中查看 LUN 的详细信息。您可以看到未向此 LUN 分配任何性能服务级别。

   JSON 输出示例

```
"assigned_performance_service_level": {
      "key": null,
      "name": "Unassigned",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
```

3. 获取要分配给 LUN 的性能服务级别的键。

类别	HTTP 谓词	路径
性能服务级别	GET	`/storage-provider/performance-service-levels`

您可以通过将 `system_defined`输入参数设置为 `true`来检索系统定义的性能服务级别的详细信息。从输出中，获取要在 LUN 上应用的性能服务级别的键。

4. 在 LUN 上应用性能服务级别。

类别	HTTP 谓词	路径
存储提供商	PATCH	`/storage-provider/lun/{key}`

在输入中，您必须仅指定要更新的参数以及 LUN 键。在本例中，它是性能服务级别的键。

示例 **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\" }"
```

JSON 输出将显示可用于验证已更新 LUN 的作业对象键。

5. 使用您获取的 LUN 密钥运行以下 API ，以查看 LUN 的详细信息。

类别	HTTP 谓词	路径
存储提供商	GET	`/storage-provider/luns/{key}`

在输出中查看 LUN 的详细信息。您可以看到性能服务级别已分配给此 LUN。

JSON 输出示例

```
    "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"
            }
```

使用 **Active IQ Unified Manager API** 修改 **NFS** 文件共享以支持 **CIFS**

您可以修改 NFS 文件共享以支持 CIFS 协议。在文件共享创建期间，可以为同一文件共享指定访问控制列表（ACL）参数和导出策略规则。但是，如果要在创建 NFS 文件共享的同一卷上启用 CIFS，则可以更新该文件共享上的 ACL 参数以支持 CIFS。

开始之前

1. 必须仅使用导出策略详细信息创建 NFS 文件共享。有关信息，请参见_管理文件共享_和_修改存储工作负载_。
2. 要运行此操作，您必须具有文件共享密钥。有关使用作业 ID 查看文件共享详细信息和检索文件共享密钥的信息，请参阅 *Provisioning CIFS and NFS file shares*。

这适用于您仅通过添加导出策略规则而不添加 ACL 参数来创建的 NFS 文件共享。您修改 NFS 文件共享以包含 ACL 参数。

步骤

1. 在 NFS 文件共享上，使用 ACL 详细信息执行 `PATCH`操作，以允许 CIFS 访问。

类别	**HTTP** 谓词	路径
storage-provider	PATCH	`/storage-provider/file-shares`

示例 **cURL**

根据您分配给用户组的访问权限（如下面的示例所示），将创建 ACL 并将其分配给文件共享。

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
```

JSON 输出示例

该操作返回运行更新的作业的作业 ID。

2. 通过查询相同文件共享的文件共享详细信息来验证参数是否已正确添加。

类别	HTTP 谓词	路径
storage-provider	GET	`/storage-provider/file-shares/{key}`

JSON 输出示例

```
"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"
        }
    }
```

您可以看到与导出策略一起分配给同一文件共享的 ACL。

法律声明

法律声明提供对版权声明、商标、专利等信息的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NETAPP、NETAPP 标识和 NetApp 商标页面上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。

"https://www.netapp.com/company/legal/trademarks/"

专利

当前 NetApp 拥有的专利列表可以在以下网址找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

开源

有关本产品中使用的第三方版权和许可的信息。

"Active IQ Unified Manager 9.18 通知"

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。